

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-149417

(43)Date of publication of application : 30.05.2000

(51)Int.Cl.

G11B 20/10
G06F 3/06
G06F 12/14
H04H 1/00
H04L 9/08
H04L 9/32

(21)Application number : 10-312596

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 02.11.1998

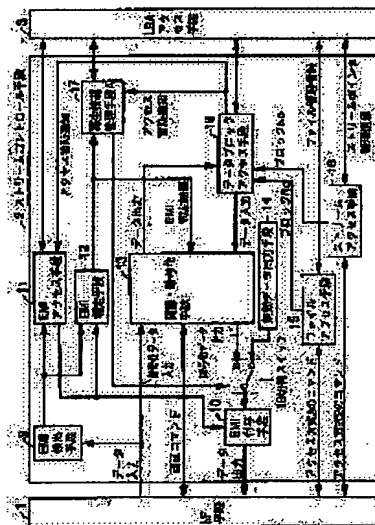
(72)Inventor : KUNO YOSHIKI
NISHIMURA TAKUYA
TAKECHI HIDEAKI
YAMADA MASAZUMI
IIZUKA HIROYUKI
GOTO SHOICHI

(54) RECORDING AND REPRODUCING DEVICE, PROGRAM RECORDING MEDIUM, AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a recording and reproducing device and a program recording medium therefor capable of transferring AV data from a once-recorded recording medium to another recording medium when utilization duplication is permitted only once by program utilization license information.

SOLUTION: This recording and reproducing device is provided with a recording means 11, 17, 18, and a reproducing means 11, 17, 18, 19 for reproducing only once an AV data recorded by the recording means 11, 17, 18 when signal information showing AV data utilization permission information represents a duplication inhibit permitting viewing and listening only one. An EMI judging means 12 judges the presence or absence and the kind of the utilization permission from the EMI information. An authenticating and enciphering means 13 performs authentication between AV apparatuses via a digital I/F means 1, and deciphers the AV data inputted from the I/F means 1, and also enciphers the AV data read from a disk medium 6 side via a data block accessing means 18.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

This Page Blank (uspto)

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-149417

(P2000-149417A)

(43)公開日 平成12年5月30日(2000.5.30)

(51)Int.Cl. ⁷	識別記号	F I	テマコード*(参考)
G 1 1 B 20/10		G 1 1 B 20/10	H 5 B 0 1 7
G 0 6 F 3/06	3 0 1	G 0 6 F 3/06	3 0 1 A 5 B 0 6 5
	12/14		3 2 0 F 5 D 0 4 4
H 0 4 H 1/00	3 2 0	H 0 4 H 1/00	F 5 J 1 0 4
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B

審査請求 未請求 請求項の数23 OL (全 32 頁) 最終頁に続く

(21)出願番号 特願平10-312596

(22)出願日 平成10年11月2日(1998.11.2)

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 久野 良樹

大阪府門真市大字門真1006番地 松下電器産業株式会社内

(72)発明者 西村 拓也

大阪府門真市大字門真1006番地 松下電器産業株式会社内

(74)代理人 100092794

弁理士 松田 正道

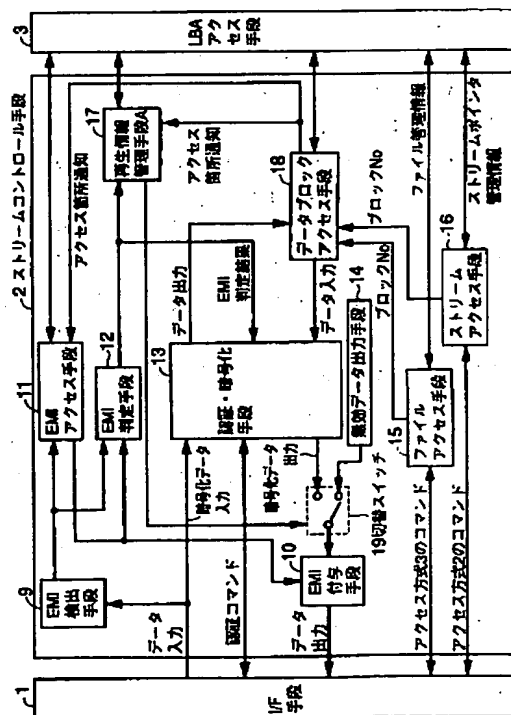
最終頁に続く

(54)【発明の名称】 記録再生装置、プログラム記録媒体及び記録媒体

(57)【要約】

【課題】 放送される番組を一回に限り視聴を許可するというのが著作権者の意図である場合に、視聴者が視聴できる時間帯まで限定されてしまう。すなわち視聴者が自分の都合のよい時間帯に番組を視聴したい場合であっても、番組が放送される時間帯にしかその番組を視聴できないという課題がある。

【解決手段】 AVデータを記録する記録手段11、17、18と、前記AVデータの利用許諾情報を示す信号情報が1回だけ視聴を許可する複製禁止(copy never)を表す場合、記録手段11、17、18により記録されたAVデータを1回だけ再生する再生手段11、17、18、19とを備えたことを特徴とする記録再生装置である。



【特許請求の範囲】

【請求項1】 AVデータを記録する記録手段と、前記AVデータの利用許諾情報を示す信号情報が1回だけ視聴することを許可する複製禁止(copy never)を表す場合、前記記録手段により記録された前記AVデータを1回だけ再生する再生手段とを備えたことを特徴とする記録再生装置。

【請求項2】 AVデータを記録する記録手段と、前記AVデータの利用許諾情報を示す信号情報が1回だけ複製することを許可する(copy one generation)ことを表す場合、前記記録手段により1回複製された後の前記AVデータの前記利用許諾情報を示す信号情報を、再び1回だけ複製することを許可する(copy one generation)ことを表して、前記AVデータを1回だけ再生する再生手段とを備えたことを特徴とする記録再生装置。

【請求項3】 前記利用許諾情報は、IEEE1394によるバケットのヘッダ内にEMIとして保持されており、IEEE1394に基づくバケットデータとして送られてくることを特徴とする請求項1または2記載の記録再生装置。

【請求項4】 前記利用許諾情報は、IEEE1394によるバケットの内部に埋め込まれているCGMSであり、IEEE1394に基づくバケットデータとして送られてくることを特徴とする請求項1または2記載の記録再生装置。

【請求項5】 前記記録手段は、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記AVデータを記録する際、未再生のデータであることを意味する再生情報を付加し、前記再生手段は、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記AVデータを再生する際、前記AVデータの再生された部分に再生済みであることを意味する前記再生情報を付加し、前記AVデータの未再生の部分と区別することを特徴とする請求項1～4のいずれかに記載の記録再生装置。

【請求項6】 前記再生手段は、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記AVデータを再生する際、記録媒体上の前記AVデータに関する配置情報を削除してそのAVデータの占有する領域を空き領域とすることを特徴とする請求項1～4のいずれかに記載の記録再生装置。

【請求項7】 前記再生手段は、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記AVデータを再生する際、前記AVデータが記録されている記録媒体上の記録部分を消去することを特徴とする請求項1～4のいずれかに記載の記録再生装置。

【請求項8】 前記記録手段は、前記AVデータと前記再生情報とを同じ領域に関連付けて記録することを特徴とする請求項5記載の記録再生装置。

【請求項9】 前記記録手段は、前記AVデータと前記再生情報とを別々の領域に関連付けて記録することを特徴とする請求項5記載の記録再生装置。

【請求項10】 前記記録手段は、前記再生情報をユーザがアクセス出来ない領域に記録することを特徴とする請求項5、8または9のいずれかに記載の記録再生装置。

【請求項11】 請求項5、8、9または10のいずれかに記載の再生情報を記録していることを特徴とする記録媒体。

【請求項12】 前記再生手段は、前記AVデータを再生する際、前記利用許諾情報が前記AVデータが複製禁止または1回だけ複製許可を表す場合、前記再生情報が前記AVデータの全部または一部が未再生であることを示すとき、その部分の前記AVデータを暗号化して出力することを特徴とする請求項5、8、9または10のいずれかに記載の記録再生装置。

【請求項13】 前記再生手段は、前記AVデータを再生する際、前記利用許諾情報が前記AVデータが複製禁止または1回だけ再生許可を表す場合、前記再生情報が前記AVデータの全部または一部が再生済であることを示すとき、その部分の前記AVデータを暗号化して出力し、かつ復号化のための鍵は出力しないことを特徴とする請求項5、8、9または10のいずれかに記載の記録再生装置。

【請求項14】 前記再生手段は、前記AVデータを再生する際、前記利用許諾情報が前記AVデータが複製禁止または1回だけ複製許可を表す場合、前記再生情報が前記AVデータの全部または一部が再生済みであることを示すとき、その部分の前記AVデータを出力しないで、無効なデータを出力することを特徴とする請求項5、8、9、10または12のいずれかに記載の記録再生装置。

【請求項15】 時間とともに変化する一連の鍵を生成する時変鍵生成手段と、前記鍵を用いて前記AVデータを暗号化する記録用暗号化手段と、暗号化された前記AVデータを復号化する再生用復号化手段とを有し、

前記AVデータを記録する際、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記記録用暗号化手段は、前記時変鍵生成手段で生成された前記鍵を用いて順次前記AVデータを暗号化し、前記記録手段は、前記鍵と前記AVデータに関連付けて記録し、

前記AVデータを再生する際、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記再生手段は、暗号化されている前記AVデータと前記鍵とを取り出し、取り出された前記鍵の記録部分を消去し、前記再生用復号化手段は、取り出された前記鍵を用いて

暗号化されている前記AVデータを復号化することを特徴とする請求項1～4のいずれかに記載の記録再生装置。

【請求項16】 前記再生手段は、前記鍵の記録部分を消去する際、記録媒体上の鍵に関する記録位置情報を削除することを特徴とする請求項15記載の記録再生装置。

【請求項17】 時間とともに変化する一連の鍵を生成する時変鍵生成手段と、

前記鍵を用いて前記AVデータを暗号化する記録用暗号化手段と、

暗号化された前記AVデータを復号化する再生用復号化手段とを有し、

前記AVデータを記録する際、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記記録用暗号化手段は、前記時変鍵生成手段で生成された前記鍵を用いて順次前記AVデータを暗号化し、

前記記録手段は、前記鍵と前記AVデータを関連付けて記録し、

前記鍵が未だ読み出されていないことを意味する鍵読み出し情報を付加して記録し、

前記AVデータを再生する際、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記再生手段は、暗号化されている前記AVデータと前記鍵とを取り出し、取り出された前記鍵が読み出し済であることを意味する前記鍵読み出し情報を付加し、

前記再生用復号化手段は、取り出された前記鍵を用いて暗号化されている前記AVデータを復号化することを特徴とする請求項1～4のいずれかに記載の記録再生装置。

【請求項18】 前記記録手段は、前記鍵または前記鍵読み出し情報を前記AVデータと同じ領域に関連付けて記録することを特徴とする請求項15または17記載の記録再生装置。

【請求項19】 前記記録手段は、前記鍵または前記鍵読み出し情報を前記AVデータと別々の領域に関連付けて記録することを特徴とする請求項15または17記載の記録再生装置。

【請求項20】 前記記録手段は、前記鍵または前記鍵読み出し情報をユーザがアクセスできない領域に記録したことを特徴とする請求項15、17、18または19のいずれかに記載の記録再生装置。

【請求項21】 前記ユーザがアクセス出来ない領域とは、LBA(logical block address)単位でアクセス出来ない領域、またはLBA単位でアクセス出来る領域を限定した領域、または交代セクタ領域、またはAVデータとして再生される領域以外の領域(AUX)、または記録媒体に付加されたRAM、または光ディスクのヘッダ領域、またはパワーキャリブレーションエリア、またはレコーディングマネジメント

エリア、またはリードインエリア、またはリードアウトエリアであることを特徴とする請求項10または20記載の記録再生装置。

【請求項22】 請求項17に記載の鍵読み出し情報を記録していることを特徴とする記録媒体。

【請求項23】 請求項1～22のいずれかに記載の記録再生装置の各構成要素の全部または一部の機能をコンピュータに実行させるためのプログラムを格納していることを特徴とするプログラム記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、AVデータにその利用許諾情報が付加されている場合の記録再生装置に関するものである。

【0002】

【従来の技術】ホーム・マルチメディア・システム、ホーム・ネットワークの要求が、デジタル化の波によって急速に高まってきている。またオフィスや業務システムにおいても家庭のシステム以上にデジタル化とマルチメディア化のニーズが高まっている。このような状況の中にあつて近年注目されているのがIEEE1394-1995である。これは、1995年にIEEEで、物理層(Physical Layer)、リンク層(Link Layer)を中心に規格化された高速シリアル・バス標準であり、100Mbps、200Mbpsおよび400Mbpsデータ転送のためのハードウェア、およびソフトウェアの標準である。IEEE1394は、プラグ&プレイやマルチメディア・データ転送のための特徴的な機能を備えている。つまりビデオや音声といったデータを転送するための帯域を確保し、リアルタイム転送を可能にするアイソクロナス・データ転送(Isochronous)を持つ。またIEEE1394バスで接続されたPCの制御プログラムからIEEE1394制御コマンド(アシンクロナス(非同期)データ)によってデジタルカメラなどの映像データの制御(映像データの切り替え、カメラの制御)を同時に行うこともできる。

【0003】このような標準であるIEEE1394-1995に基づいて行うAVデータの利用許諾情報には、CGMSがある。CGMSは放送局から送られてくるトランスポートストリームの内部に存在している。CGMSは2ビットのデータであり、CGMSの取りうる値とその意味は次のようになる。

【0004】すなわちCGMS=11のときcopy neverを意味し、CGMS=10のときcopy one generationを意味し、CGMS=00のときcopy freeを意味する。ただしcopy neverは複製禁止のことであり、そのAVデータを1回だけ視聴することを許可するものである。copy one generationは1世代のみ

複製を許可するものであり、複製したAVデータは何度でも繰り返して視聴することができるものである。copy freeは自由に複製してよいことを示すものである。

【0005】CGMSが11のときすなわちcopy neverのとき、AVデータは一回だけ視聴することが出来る。すなわちそのAVデータが放送されている時間帯に限ってそのAVデータを視聴することができる。

【0006】

【発明が解決しようとする課題】しかし、従来、CGMSによる利用許諾情報がcopy neverの場合は該当するAVデータを一回だけ視聴することができるが、視聴できる時間帯は番組が放送されている時間帯に限られていた。このように一回だけ視聴を許可するというのが著作権者の意図である場合に視聴できる時間帯まで限定されてしまう。すなわち視聴者が自分の都合のよい時間帯に番組を視聴したい場合であっても、番組が放送される時間帯にしかその番組を視聴できないという課題がある。

【0007】またCGMSによる利用許諾情報がcopy one generationの場合に、一度ある記録媒体に記録してしまうと、その他の記録媒体へAVデータを移動することができないという課題がある。

【0008】本発明は番組の利用許諾情報を表す情報が複製禁止の場合に、一回だけ視聴を許可するという著作権者の意図通りに視聴者がAVデータを視聴でき、かつそのAVデータが放送された以後で時間帯を限定されずにそのAVデータを視聴者が視聴できる記録再生装置及びプログラム記録媒体を提供することを目的とするものである。

【0009】また本発明は番組の利用許諾情報が一回だけ複製を許可する場合に、一度記録した記録媒体から別の記録媒体へAVデータの移動を行うことが出来る記録再生装置及びプログラム記録媒体を提供することを目的とするものである。

【0010】

【課題を解決するための手段】上述した課題を解決するために、第1の本発明（請求項1に対応）は、AVデータを記録する記録手段と、前記AVデータの利用許諾情報を示す信号情報が1回だけ視聴することを許可する複製禁止（copy never）を表す場合、前記記録手段により記録された前記AVデータを1回だけ再生する再生手段とを備えたことを特徴とする記録再生装置である。

【0011】また第2の本発明（請求項2に対応）は、AVデータを記録する記録手段と、前記AVデータの利用許諾情報を示す信号情報が1回だけ複製することを許可する（copy one generation）ことを表す場合、前記記録手段により1回複製された後の前記AVデータの前記利用許諾情報を示す信号情報を、

再び1回だけ複製することを許可する（copy one generation）ことを表して、前記AVデータを1回だけ再生する再生手段とを備えたことを特徴とする記録再生装置である。

【0012】また第3の本発明（請求項3に対応）は、前記利用許諾情報は、IEEE1394によるパケットのヘッダ内にEMIとして保持されており、IEEE1394に基づくパケットデータとして送られてくることを特徴とする第1または2の発明に記載の記録再生装置である。

【0013】また第4の本発明（請求項4に対応）は、前記利用許諾情報は、IEEE1394によるパケットの内部に埋め込まれているCGMSであり、IEEE1394に基づくパケットデータとして送られてくることを特徴とする第1または2の発明に記載の記録再生装置である。

【0014】また第5の本発明（請求項5に対応）は、前記記録手段は、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記AVデータを記録する際、未再生のデータであることを意味する再生情報を付加し、前記再生手段は、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記AVデータを再生する際、前記AVデータの再生された部分に再生済みであることを意味する前記再生情報を付加し、前記AVデータの未再生の部分と区別することを特徴とする第1～4の発明のいずれかに記載の記録再生装置である。

【0015】また第6の本発明（請求項6に対応）は、前記再生手段は、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記AVデータを再生する際、記録媒体上の前記AVデータに関する配置情報を削除してそのAVデータの占有する領域を空き領域とすることを特徴とする第1～4の発明のいずれかに記載の記録再生装置である。

【0016】また第7の本発明（請求項7に対応）は、前記再生手段は、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記AVデータを再生する際、前記AVデータが記録されている記録媒体上の記録部分を消去することを特徴とする第1～4の発明のいずれかに記載の記録再生装置である。

【0017】また第8の本発明（請求項8に対応）は、前記記録手段は、前記AVデータと前記再生情報とを同じ領域に関連付けて記録することを特徴とする第5の発明に記載の記録再生装置である。

【0018】また第9の本発明（請求項9に対応）は、前記記録手段は、前記AVデータと前記再生情報とを別々の領域に関連付けて記録することを特徴とする第5の発明に記載の記録再生装置である。

【0019】また第10の本発明（請求項10に対応）は、前記記録手段は、前記再生情報をユーザがアクセス出来ない領域に記録することを特徴とする第5、8また

は9の発明のいずれかに記載の記録再生装置である。

【0020】また第11の本発明(請求項11に対応)は、第5、8、9または10の発明のいずれかに記載の再生情報を記録していることを特徴とする記録媒体である。

【0021】また第12の本発明(請求項12に対応)は、前記再生手段は、前記AVデータを再生する際、前記利用許諾情報が前記AVデータが複製禁止または1回だけ複製許可を表す場合、前記再生情報が前記AVデータの全部または一部が未再生であることを示すとき、その部分の前記AVデータを暗号化して出力することを特徴とする第5、8、9または10の発明のいずれかに記載の記録再生装置である。

【0022】また第13の本発明(請求項13に対応)は、前記再生手段は、前記AVデータを再生する際、前記利用許諾情報が前記AVデータが複製禁止または1回だけ再生許可を表す場合、前記再生情報が前記AVデータの全部または一部が再生済であることを示すとき、その部分の前記AVデータを暗号化して出力し、かつ復号化のための鍵は出力しないことを特徴とする第5、8、9または10の発明のいずれかに記載の記録再生装置である。

【0023】また第14の本発明(請求項14に対応)は、前記再生手段は、前記AVデータを再生する際、前記利用許諾情報が前記AVデータが複製禁止または1回だけ複製許可を表す場合、前記再生情報が前記AVデータの全部または一部が再生済みであることを示すとき、その部分の前記AVデータを出力しないで、無効なデータを出力することを特徴とする第5、8、9、10または12の発明のいずれかに記載の記録再生装置である。

【0024】第15の本発明(請求項15に対応)は、時間とともに変化する一連の鍵を生成する時変鍵生成手段と、前記鍵を用いて前記AVデータを暗号化する記録用暗号化手段と、暗号化された前記AVデータを復号化する再生用復号化手段とを有し、前記AVデータを記録する際、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記記録用暗号化手段は、前記時変鍵生成手段で生成された前記鍵を用いて順次前記AVデータを暗号化し、前記記録手段は、前記鍵と前記AVデータを関連付けて記録し、前記AVデータを再生する際、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記再生手段は、暗号化されている前記AVデータと前記鍵とを取り出し、取り出された前記鍵の記録部分を消去し、前記再生用復号化手段は、取り出された前記鍵を用いて暗号化されている前記AVデータを復号化することを特徴とする第1～4の発明のいずれかに記載の記録再生装置である。

【0025】また第16の本発明(請求項16に対応)は、前記再生手段は、前記鍵の記録部分を消去する際、

記録媒体上の鍵に関する記録位置情報を削除することを特徴とする請求項15記載の記録再生装置である。

【0026】また第17の本発明(請求項17に対応)は、時間とともに変化する一連の鍵を生成する時変鍵生成手段と、前記鍵を用いて前記AVデータを暗号化する記録用暗号化手段と、暗号化された前記AVデータを復号化する再生用復号化手段とを有し、前記AVデータを記録する際、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記記録用暗号化手段は、前記時変鍵生成手段で生成された前記鍵を用いて順次前記AVデータを暗号化し、前記記録手段は、前記鍵と前記AVデータを関連付けて記録し、前記鍵が未だ読み出されていないことを意味する鍵読み出し情報を付加して記録し、前記AVデータを再生する際、前記利用許諾情報が複製禁止または1回だけ複製許可を表す場合、前記再生手段は、暗号化されている前記AVデータと前記鍵とを取り出し、取り出された前記鍵が読み出し済であることを意味する前記鍵読み出し情報を付加し、前記再生用復号化手段は、取り出された前記鍵を用いて暗号化されている前記AVデータを復号化することを特徴とする第1～4の発明のいずれかに記載の記録再生装置である。

【0027】また第18の本発明(請求項18に対応)は、前記記録手段は、前記鍵または前記鍵読み出し情報を前記AVデータと同じ領域に関連付けて記録することを特徴とする第15または17の発明に記載の記録再生装置である。

【0028】また第19の本発明(請求項19に対応)は、前記記録手段は、前記鍵または前記鍵読み出し情報を前記AVデータと別々の領域に関連付けて記録することを特徴とする第15または17の発明に記載の記録再生装置である。

【0029】また第20の本発明(請求項20に対応)は、前記記録手段は、前記鍵または前記鍵読み出し情報をユーザがアクセスできない領域に記録したことを特徴とする第15、17、18または19の発明のいずれかに記載の記録再生装置である。

【0030】また第21の本発明(請求項21に対応)は、前記ユーザがアクセス出来ない領域とは、LBA(logical block address)単位でアクセス出来ない領域、またはLBA単位でアクセス出来る領域を限定した領域、または交代セクタ領域、またはAVデータとして再生される領域以外の領域(AUX)、または記録媒体に付加されたRAM、または光ディスクのヘッダ領域、またはパワーキャリブレーションエリア、またはレコーディングマネージメントエリア、またはリードインエリア、またはリードアウトエリアであることを特徴とする第10または20の発明に記載の記録再生装置である。

【0031】また第22の本発明(請求項22に対応)は、第17の発明に記載の鍵読み出し情報を記録してい

ることを特徴とする記録媒体である。

【0032】第23の本発明(請求項23に対応)は、第1～22の発明のいずれかに記載の記録再生装置の各構成要素の全部または一部の機能をコンピュータに実行させるためのプログラムを格納していることを特徴とするプログラム記録媒体である。

【0033】

【発明の実施の形態】以下に、本発明の実施の形態について図面を参照して説明する。

【0034】(実施の形態1)まず第1の実施の形態について説明する。

【0035】本実施の形態では、放送局から送られてくるAVデータの利用許諾情報が複製禁止を意味するcopy neverである場合に、放送が行われた時間帯以後の任意の時間にその番組を一回だけ視聴できる記録再生装置の例としてハードディスク装置について説明する。本実施の形態では、利用許諾情報がcopy neverであるAVデータを記録可能とし、再生情報管理手段を用いてそのAVデータを一回しか再生できないようにすることでこのようなハードディスク装置を実現した。また本実施の形態で使用する再生情報はディスク媒体上でデータブロックとは別の領域に記録されている場合を説明する。

【0036】図1は本発明のハードディスク装置の基本構成図である。

【0037】ハードディスク装置は、デジタルI/F手段1、ストリームコントロール手段2、LBAアクセス手段3、ハードディスクコントロール手段4、アクチュエータ手段5、ディスク媒体6、ヘッド7、スピンドルモータ手段8から構成される。

【0038】デジタルI/F手段1は、STB(Set Top Box; 衛星放送受信器)、テレビモニタ、DVHS、ハードディスク装置など外部AV機器間を接続し、AV機器のコントロールとAVデータの転送を行う手段であり、例えばIEEE1394-1995に記述されているIEEE standard for High performance Serial Busである。デジタルI/F手段1のAVデータの転送は、アイソクロナス(Isochronous)方式と呼ばれる転送方式で行われ、転送されるデータのリアルタイム性を保証しながら転送処理が行える。転送されるデータとしては例えばMPEGトランスポートストリームやDVストリームなどがある。またデジタルI/F手段1のAV機器のコントロールは、アシンクロナス(Asynchronous)方式と呼ばれる非同期な転送方式で行われる。ストリームコントロール手段2は、ストリームのアクセスや認証処理を行う手段である。LBAアクセス手段は、LBA(logical block address)を指定してディスク媒体へアクセスするためのハードディスク装置内部のI/F手段である。ハ

ードディスクコントロール手段4は、アクチュエータ手段5、スピンドルモータ手段8を制御し、またヘッド7を経由してディスク媒体6に対して記録再生をするための信号処理を行う手段である。ヘッド7は、ディスク媒体6に対して信号を記録再生するための手段である。スピンドルモータ手段8は、ディスク媒体を一定の速度で回転させる手段である。アクチュエータ手段5は、ディスク媒体6の目的とする位置へヘッド7を位置決めするための手段である。

【0039】本実施の形態では、利用許諾情報としてCGMSから生成されるEMI(Encryption Mode Indicator)を使用するので、EMIに関して説明しておく。

【0040】まずその前にデジタルI/F手段1を説明したときに若干触れたが、IEEE1394のデータ転送プロトコルについて簡単に説明する。AVデータをモニタで視聴しているときには、データを周期的に同期して送信する必要があり、またハードディスク装置などの停止や録画開始などを制御するときには、制御コマンドを非同期で任意のタイミングで送受信ができる必要がある。IEEE1394では、前者のデータとして、アイソクロナス・パケットデータがあり、後者のデータとして、アシンクロナス・パケットデータがある。

【0041】データ転送では、転送に先立って管理ノードにバス使用権を要求し、使用許諾権を得る。

【0042】アシンクロナス転送では、送信ノードIDと受信ノードIDが転送データと一緒にパケット・データとして送られる。受信ノードは自分のIDを確認してパケットを受け取るとアクノリッジ信号を送信ノードに返す。これで一つのトランザクションが終わる。

【0043】アイソクロナス転送では、送信ノード側で伝送速度と一緒にアイソクロナス・チャンネルを要求する。チャンネルIDが転送データと一緒にパケット・データとして送られる。受信ノードは自分が欲しいチャンネルIDを確認してパケットを受け取る。

【0044】以上でIEEE1394のデータ転送プロトコルについて簡単に説明した。

【0045】さて、EMIの説明に戻る。CGMSは、放送局でAVデータに付加される。放送局から送られてくる放送波を受信したSTBはIEEE1394バスに受信した番組を流す。この時CGMSはアイソクロナス・パケットデータのMPEGトランスポートストリームのサービス情報の部分に埋め込まれる。一つのアイソクロナス・パケットデータには複数のMPEGデータが格納されており、各MPEGデータに対して、それぞれ対応するCGMSが存在する。

【0046】EMIはこのようなCGMSからSTBによって生成される。STBは一つのアイソクロナス・パケットデータで送信する各AVデータのCGMSを調べその代表値として一つのアイソクロナス・パケットデー

タに一つのEMIを付与する。そのEMIはアイソクロナス・パケットデータのヘッダ部分に保持される。

【0047】CGMSは、次の値をとる。すなわち、CGMS=11が複製禁止(copy never)を表し、CGMS=10が一世代のみ複製を許可(copy one generation)を表し、CGMS=00が複製自由(copy free)を表す。

【0048】EMIの取る値は、一つのアイソクロナス・パケットデータの中に存在するAVデータのCGMSのうちで、利用許諾条件の制限が最も厳しいCGMSの値をとる。例えば、一つのアイソクロナス・パケットデータの中のAVデータのCGMSが11、10、10であったとすると、EMIの値は最も制限が厳しい11になる。またCGMSが10、10、00、00である場合は、EMIの値はその中で最も制限が厳しい10となる。このようにしてEMIの値が決定される。

【0049】EMIの取り得る値は、EMI=11が複製禁止(copy never)を表し、EMI=10が一世代のみ複製を許可(copy one generation)を表し、EMI=00が複製自由(copy free)を表す。ここまでは、CGMSと同じである。EMIだけのものとして、EMI=01があつて、これはcopy one generationのAVデータを記録した後にEMIが変更されたもので、これ以上の複製は不許可(no more copy)を表す。

【0050】以上でEMIについて説明した。

【0051】図1に戻って、ハードディスク装置のストリームコントロール手段2は、図2のように構成される。すなわちストリームコントロール手段2は、EMI検出手段9、EMI付与手段10、EMIアクセス手段11、EMI判定手段12、認証・暗号化手段13、無効データ出力手段14、ファイルアクセス手段15、ストリームアクセス手段16、再生情報管理手段A17、データブロックアクセス手段18、切替スイッチ19から構成される。

【0052】EMI検出手段9は、デジタルI/F手段1から入力したアイソクロナス・パケットデータ中のヘッダ部分からEMIを記述したフィールドを検出する手段である。EMI付与手段10は、デジタルI/F手段1へ出力するアイソクロナス・パケットデータ中のヘッダ部分に指示されたEMIを付与する手段である。EMIアクセス手段11は、検出したEMI情報をLBAアクセス手段3を経由して読み出し、さらに検出したEMI情報を指定されたデータブロックに対応して記録再生する手段である。EMI判定手段12は、EMI情報から利用許諾の有無と種類を判定する手段である。認証・暗号化手段13は、デジタルI/F手段1を介してAV機器間の認証を行い、またデジタルI/F手段1から入力されるAVデータを復号化し、またディスク媒体6側

からデータブロックアクセス手段18を経由して読み出されたAVデータを暗号化する手段である。データブロックアクセス手段18は、指定されたブロック番号のデータをLBAアクセス手段3を経由して記録または再生を行い、また現在どのブロック番号をアクセス中であるかをEMIアクセス手段11と再生情報管理手段A17に通知する手段である。ストリームアクセス手段16は、デジタルI/F手段1から受信されるアクセス方式2のコマンドを実行するためにデータブロックアクセス手段18に記録または再生するブロック番号を指定し、またディスク媒体6のユーザ領域を先頭データブロックから最終データブロックまで1本のテープのように見立てて、再生、記録、停止等の指示に従い、ストリームが現在どのブロック位置にいるかを示すストリームポインタ管理を行い、またストリームポインタ管理情報をLBAアクセス手段3を経由してディスク媒体6に対して記録または読み出しを行う手段である。ここで、アクセス方式2とは、例えばAV/C Digital Interface Command Set VCR subunit Specification version 2.0.1に準拠した方式である。ファイルアクセス手段15は、デジタルI/F手段1から受信されるアクセス方式3のコマンドを実行するためにデータブロックアクセス手段18に記録または再生するブロック番号を指定し、またファイル管理情報を有し、ファイル名とそのファイルを構成する複数のデータブロックの順序構成を管理し、またアクセス方式3のコマンドに従って、再生、記録、停止等の指示に従い、現在ファイル中のどのブロック位置にいるかを示すファイルポインタも管理し、またこれらのファイルのデータブロックの順序構成情報や、ファイルポインタ情報等をLBAアクセス手段3を経由してディスク媒体6に対して記録または読み出しを行う手段である。ここで、アクセス方式3とは、例えばAV/C Digital Interface Command Set General Specificationに準拠して、ファイル名とそのファイルに対する処理内容、再生、記録、停止等を指示することによってAV装置をコントロールするアクセス方式である。切替スイッチ19は、EMI付与手段10を経由して、デジタルI/F手段1にAVデータを出力する際に、再生情報管理手段A17の結果により、再生済みの場合には、スイッチをoffにするかまたは無効データ出力手段14に切り替えて、ブルーバックや黒画面などの無効データを出力し、未再生の場合には、スイッチを認証・暗号化手段13に切り替えて暗号化されたAVデータを出力する手段である。再生情報管理手段A17は、指定されたデータブロックに対応した再生情報を記録、読み出しし、また再生情報から再生済みかどうか判断する手段である。

【0053】図2の認証・暗号化手段13は図3のよう

に構成される。すなわち復号化手段20、認証手段21、鍵生成手段22、暗号化手段23、切替スイッチ24、切替スイッチ25から構成される。

【0054】認証手段21は、デジタルI/F手段1間を接続するAV装置間で相互に認証を行い、認証が成功すると、デジタルI/F側にAVデータを出力したい場合、自分が暗号化に使用したときの鍵を相手に渡し、デジタルI/F手段1側からAVデータを入力したい場合、自分が復号化に使用する鍵を相手からもらう手段である。暗号化手段23は、データブロックアクセス手段18を経由してディスク媒体6から読み出されたAVデータを鍵生成手段22により生成された鍵を用いて暗号化してデジタルI/F手段1に出力する手段である。鍵生成手段22は暗号化のために使用する鍵を生成し、暗号化手段23と認証手段21に渡す手段である。復号化手段20は、デジタルI/F手段1から入力される暗号化されたAVデータを認証手段21で得られた鍵を用いて復号化し、データブロックアクセス手段18に出力する手段である。スイッチ24、25は、EMI判定手段12の判定結果に対してEMIが00のときは、入出力データを暗号化手段23及び復号化手段20を経由しないように切り替え、EMIが00以外のときは、入出力データが暗号化手段23及び復号化手段20を経由するように切り替える手段である。

【0055】また図2の再生情報管理手段A17は図4のように構成される。すなわち再生情報更新手段26、再生済判定手段27、再生情報生成手段28、再生情報アクセス手段29、切替スイッチ30から構成される。

【0056】再生情報生成手段28は、再生情報を生成する手段であり、例えば再生済みフラグplay_flagを0で初期化する手段である。play_flagが0の場合は、該当するAVデータがまだ再生されていないことを表すものとする。再生情報更新手段26は、再生情報を更新し、データが再生済みであるという情報に更新する手段である。例えば再生済みフラグplay_flagを1で更新する手段である。play_flagが1の場合は、該当するAVデータがすでに再生されていることを表すものとする。再生情報アクセス手段29は、各データブロックに対応する再生情報をテーブルで記憶し、LBAアクセス手段3を経由してディスク媒体6に再生情報を記録または読み出しを行う手段である。再生済判定手段27は、再生情報アクセス手段29が読み出した再生情報に基づいて、再生済みであるかどうかを判定する手段である。例えば再生済みフラグplay_flagが1ならば既に1回再生されたと判断し、またEMI判定結果を使ってEMIが11のcopy_neverの場合、未再生と判断したらスイッチ30を切り替えて、再生情報(再生済みフラグ)を更新させる手段である。スイッチ30は、再生済み判定手段27で新規にAVデータを記録すると判定されたら、再生

情報生成手段28の側に切り替え、また再生時などでAVデータがすでに記録されていると判定されたら、再生情報更新手段26の側に切り替える手段である。

【0057】次にこのような本実施の形態の動作について説明する。

【0058】AVデータを送ってくるものと装置としてSTBを考えることにする。また、IEEE1394バスで結合された装置に番組受信命令や、記録開始命令、記録停止命令等を送るコントローラが存在するが、コントローラとハードディスク装置及びSTBとのコマンドのやりとりを記述することは、本実施の形態の本旨からそれるので、本実施の形態では記述を省略する。

【0059】まずコントローラが、STBに放送局から送られてくる番組の受信を開始する受信開始コマンドを送り、かつハードディスク装置に記録開始コマンドを送ったとする。STB以外の装置、例えばDVHSやハードディスク装置などの記録再生装置から送られてくるAVデータを受信する場合は後述する。そうすると放送局から送られて来た番組はSTBによって受信され、EMIを付与されたあとアイソクロナス・パケットデータとしてIEEE1394バスに送られる。またハードディスク装置は、デジタルI/F手段1からアクセス方式2またはアクセス方式3のコマンドで記録開始コマンドを受信すると、デジタルI/F手段1は自分が欲しいチャンネル番号を確認して、該当するアイソクロナス・パケットデータを取り込む。今、アクセス方式2のコマンドで記録開始コマンドを受信したとする。そうすると認証手段21はSTBに認証コマンドを送る。EMI検出手段9は、取り込まれたアイソクロナス・パケットデータのヘッダ部分に保持されているEMI情報を検出する。EMI判定手段12は、検出したEMI情報から利用許諾の有無とその種類を判定する。その結果は認証・暗号化手段13に入力され、認証手段21は、利用許諾の有無とその種類によって認証方法を決める。EMIが11のとき、すなわちcopy_neverの場合は、AVデータの重要度は高いので、公開鍵による認証を行う。またEMIが10のとき、すなわちcopy_one_generationのときは、AVデータの重要度はEMIが11の場合よりは高くないので、共通鍵による認証を行う。またEMIが00のとき、すなわちcopy_freeのときは、AVデータは重要でないので、認証を行わないで、認証が成功したものとみなす。STBは認証コマンドを受信すると、ハードディスク装置との間で公開鍵または共通鍵による認証を行い、認証が成功すると、ハードディスク装置に鍵を渡す。認証手段21は、デジタルI/F手段1を介して、ハードディスク装置から送られてきた鍵を受け取り、復号化手段20に渡す。ただしEMIが00のときは、認証手段21はSTBからの鍵を受け取らない。この場合はAVデータ自体が暗号化されない。EMIが11の場合とEMIが10

の場合は復号化手段20は、認証手段21から鍵を受け取る。さて、デジタルI/F手段1を介して、アクセス方式2のコマンドで、記録コマンドを受信したとする。これ以後の処理を図10のフローチャート図を参照して説明する。デジタルI/F手段1を介して、切替スイッチ24は、送られてくるAVデータのEMIが00でない場合、AVデータが復号化手段20を経由するように切り替える。また切替スイッチ24は、EMIが00の場合、AVデータが復号化手段20を経由しないように切り替える。そして復号化手段20は、受け取った鍵を用いて暗号化されているAVデータを復号化する。ストリームアクセス手段16は、データブロックアクセス手段18にブロックxの記録を指示する。データブロックアクセス手段18は、EMIアクセス手段11に現在アクセス中のブロック番号(=x)を通知する。EMIアクセス手段11は、EMI検出手段9で検出されたEMI情報を、通知されたブロック番号に対応付けて記録する。ただしEMIが10すなわちcopy one generationの場合はディスク媒体6にEMI情報を記録する際にEMIを01すなわちnomore copyに書き替えて記録する。またデータブロックアクセス手段18は、再生情報管理手段A17に現在アクセス中のブロック番号(=x)を通知する。切替スイッチ30は、記録時には再生情報生成手段28の側にスイッチを切り替える。再生情報アクセス手段29は通知されたブロック番号(=x)に対応付けて、再生情報をテーブルにして記憶する。再生情報生成手段28は、データが未再生であるという情報を再生情報に登録する。すなわちplay_flag=0で再生情報を初期化する(S1)。次に再生情報アクセス手段29は、LBAアクセス手段3を経由してディスク媒体6に再生情報を記録する(S2)。次にブロック番号を1だけ増加する。すなわちx=x+1とする(S3)。次にデジタルI/F手段1から別のコマンドの受信があるかどうか判定する(S4)。別のコマンドを受信していれば処理は終了する。そうでない場合は記録コマンドを受信してからの処理を別のコマンドの受信があるまで繰り返し行う。以上がAVデータをディスク媒体6に記録する場合である。

【0060】次にハードディスク装置が、AVデータを再生する場合を説明する。AVデータをテレビモニタに再生する場合を考える。さらにハードディスク装置に記録されているAVデータはSTBから記録されたものとする。また、IEEE1394バスで結合された装置に再生開始命令、再生停止命令等を送るコントローラが存在するが、コントローラとハードディスク装置及びテレビモニタとのコマンドのやりとりを記述することは、本実施の形態の本旨からそれるので、本実施の形態では記述を省略する。

【0061】まずコントローラが、テレビモニタに再生

開始コマンドを送り、ハードディスク装置にも再生開始コマンドを送る。そうするとハードディスク装置は、データブロックアクセス手段18が再生情報管理手段A17とEMIアクセス手段11にアクセス箇所を通知する。EMIアクセス手段11は、通知されたアクセス箇所のEMI情報を取り出し、EMI付与手段10にEMI情報を渡す。切替スイッチ19は、無効データ出力手段14の側に切り替えられ、ブルーバック画面や黒画面などの無効なデータがEMI付与手段10に渡される。EMI付与手段10は、EMIアクセス手段11から渡されたEMI情報と無効データ出力手段14から渡されたAVデータをデジタルI/F手段1を介して、アイソクロナス・パケットデータとしてIEEE1394バスに送る。テレビモニタは、ハードディスク装置に対して認証コマンドを送る。さらにテレビモニタはハードディスク装置から送られるアイソクロナス・パケットデータを取り込み、そこに付与されているEMI情報を参照して、認証方法を決定する。EMIが11つまりcopy neverの場合、認証手段21はデジタルI/F手段1を介して、テレビモニタと公開鍵による認証を行う。また、EMIが01つまりno more copyの場合、認証手段21はデジタルI/F手段1を介して、テレビモニタと共通鍵による認証を行う。またEMIが00の場合は認証は行わないで、成功したものとみなす。本実施の形態ではSTBから送られてきたAVデータを記録したものを再生する場合を扱っているので、EMIが10すなわちcopy one generationのAVデータはすべてEMIが01に書き換えられて記録されている。ハードディスク装置はデジタルI/F手段1を介して認証コマンドを受け取ると、認証手段21はEMI情報を参照して、認証の種類を決定し、テレビモニタと認証を行う。認証が成功すると、認証手段21は、鍵生成手段22で生成された鍵を暗号化手段23に渡す。EMIが00の場合は暗号化手段23に鍵を渡さず、切替スイッチ25を暗号化手段23を経由しない側に切り替える。また、切替スイッチ19は、認証・暗号化手段13の側に切り替えられる。

【0062】以後の動作は再生情報管理手段A17でいつ再生情報を更新するかで二通りの動作を行うことができる。第1の場合は、再生終了後にまとめて再生情報を更新する場合であり、第2の場合は、再生中にブロックごとに再生情報を更新する場合である。

【0063】まず第1の場合を図10のフローチャート図を参照して説明する。

【0064】ハードディスク装置は、デジタルI/F手段1からアクセス方式2のコマンドで再生コマンドを受信したとする。ストリームアクセス手段16は、データブロックアクセス手段18にブロックxの再生を指示する。データブロックアクセス手段18は、EMIアクセス手段11と、再生情報管理手段A17に、現在アクセ

ス中のブロック番号 (=x) を通知する。同時にデータブロックアクセス手段18は、LBAアクセス手段3を介してディスク媒体6からAVデータを読み出す(S5)。EMIアクセス手段11は、通知されたブロック番号に対応するEMI情報をディスク媒体6から読み出す。読み出されたEMI情報はEMI判定手段12で判定され、その判定結果は、認証・暗号化手段13と、再生済判定手段27に送られる。

【0065】EMI判定結果でEMIが00の場合(S6)は切替スイッチ25が暗号化手段23を経由しない側に切り替えられ、AVデータは暗号化されないで出力される(S8)。またEMIが00でない場合(S6)は切替スイッチ25は暗号化手段23を経由する側に切り替えられる。切替スイッチ30は、再生時には再生情報更新手段26の側にスイッチを切り替える。再生済判定手段27は、読み出されたEMI情報の判定結果を調べる。

【0066】EMIが11の場合、再生済み判定手段27は、AVデータが未再生であるか再生済みであるかを判定する(S7)。EMIが11のcopy neverであって、かつ再生済みである場合は、切替スイッチ19が無効データ出力手段14の側に切り替えられブルーバック画面や黒画面などの無効なデータが出力される(S10)。EMIが11のcopy neverであって、データが未再生の場合またはEMIが11でない場合、切替スイッチ19は認証・暗号化手段13の側に切り替えられ、AVデータは暗号化手段23で暗号化されて、デジタルI/F手段1を介して出力される(S8)。

【0067】次にブロック番号を1だけ増加する。すなわち $x = x + 1$ とする(S9)。次にデジタルI/F手段1から別のコマンドの受信があるかどうか判定する

(S11)。別のコマンドを受信していれば処理は終了する。再生処理が終了したら、再生情報アクセス手段29で再生したブロックの初期値の番号から最終値の番号までの再生情報をアクセスし、再生情報更新手段26で再生済みすなわちplay_flag=1に更新する

(S12)。そうでない場合は再生コマンドを受信してからの処理を別のコマンドの受信があるまで繰り返し行う。以上が第1の場合でAVデータを再生する場合である。

【0068】次に第2の場合を図11のフローチャート図を参照して説明する。

【0069】ハードディスク装置は、デジタルI/F手段1からアクセス方式2のコマンドで再生コマンドを受信したとする。ストリームアクセス手段16は、データブロックアクセス手段18にブロックxの再生を指示する。データブロックアクセス手段18は、EMIアクセス手段11と、再生情報管理手段A17に現在アクセス中のブロック番号 (=x) を通知する。同時にデータブ

ロックアクセス手段18は、LBAアクセス手段3を介してディスク媒体6からAVデータを読み出す(S17)。EMIアクセス手段11は、通知されたブロック番号に対応するEMI情報をディスク媒体6から読み出す。読み出されたEMI情報はEMI判定手段12で判定され、その判定結果は、認証・暗号化手段13と、再生済判定手段27に送られる。

【0070】EMI判定結果でEMIが00の場合(S18)は切替スイッチ25が暗号化手段23を経由しない側に切り替えられ、AVデータは、認証。暗号化手段13を経由し、デジタルI/F手段1を経由して、暗号化されないで出力される(S21)。またEMIが00でない場合(S18)は切替スイッチ25は暗号化手段23を経由する側に切り替えられる。切替スイッチ30は、再生時には再生情報更新手段26の側にスイッチを切り替える。再生済判定手段27は、読み出されたEMI情報の判定結果を調べる。

【0071】EMIが00でない場合、AVデータが未再生であるか再生済みであるかを判定する(S19)。EMIが11のcopy neverであって、かつ再生済みすなわちplay_flag=1である場合は、切替スイッチ19が無効データ出力手段14の側に切り替えられブルーバック画面や黒画面などの無効なデータが出力される(S22)。再生済判定手段27で、EMIが11のcopy neverであってかつデータが未再生であるすなわちplay_flag=0と判定された場合、再生情報更新手段26が再生情報をデータが再生済みにすなわちplay_flag=1に更新する

(S20)。次に切替スイッチ19は認証・暗号化手段13の側に切り替えられ、データブロックアクセス手段18で読み出されたAVデータは、暗号化手段23で暗号化されて、デジタルI/F手段1を介して出力される(S21)。さらに再生情報アクセス手段29でブロックxの再生情報を更新する(S23)。次にブロックxをx+1とおき(S24)、再生コマンド以外のコマンドを受信したら(S25)処理を終了する。そうでない場合は再生コマンドを受信してからの処理を別のコマンドの受信があるまで繰り返し行う。

【0072】以上が第2の場合でAVデータを再生する場合である。

【0073】ハードディスクに記録されたAVデータのEMIが11すなわちcopy neverである場合に、再生情報管理手段A17による判定で切替スイッチ19を切り替えることと、再生情報管理手段A17で再生情報を管理することにより、copy neverのAVデータを一回だけ再生することができる。

【0074】なお、本実施の形態では、アクセス方式2によってストリームアクセス手段16でコマンドを実行する場合を説明したが、これに限らずアクセス方式3によってファイルアクセス手段15でコマンドを実行して

もよい。この場合、記録再生の順序はブロック番号の順序ではなく、ファイル管理情報によって管理するブロックの順序に依存する。つまりx番目に記録再生するブロックをf(x)とすると、図10、図11のブロックxの記述部分はブロックf(x)で置き換えさえすればよい。

【0075】さて、EMIに対応して認証の方式を選択して実施することも可能である。すなわち認証の方式を2通り用いる。EMIが11のcopy neverに対する認証方式として方式Aの認証を用いる。またEMIが10のcopy one generationとEMIが01のno more copyに対する認証方式として方式Bの認証を用いる。具体的には方式Aの認証として公開鍵による認証、方式Bの認証として共通鍵による認証を用いることができる。そしてテレビモニタやSTBなどのAVデータを記録しない装置は方式Aと方式Bの両方の認証をサポートし、VTRなどのAVデータを記録する装置は方式Bの認証のみサポートする。さらに本発明のハードディスク装置は方式Aと方式Bの両方の認証をサポートする。本発明のハードディスク装置が、STBから送られてくるAVデータを記録したとする。STBと本発明のハードディスク装置は方式Aと方式Bの両方の認証をサポートしているので、EMIが00でない場合に認証は成功し、AVデータを本発明のハードディスク装置に記録することができる。本発明のハードディスク装置の再生時に、テレビモニタにAVデータを再生する場合、EMIが11のcopy neverであれば、テレビモニタは方式Aの認証をサポートしているので、認証が成功し、AVデータをテレビモニタに出力することができる。テレビモニタはAVデータを記録しないので、copy neverの利用許諾を守ることができる。またEMIが10のcopy one generationかEMIが01のno more copyの場合もテレビモニタは、方式Bの認証をサポートしているので、認証が成功し、AVデータをテレビモニタに出力することができる。ところがVTRにEMIが11のcopy neverのAVデータを出力する場合は、本発明のハードディスク装置は方式Aの認証を行おうとする。ところがVTRは方式Bの認証しかサポートしていないので、認証は失敗する。従ってEMIが11のAVデータはVTRに記録することはできない。ところが、EMIが10のcopy one generationかEMIが01のno more copyの場合は、方式Bの認証を行うことになる。VTRは方式Bの認証をサポートしているので、認証は成功する。EMIが10のcopy one generationの場合はVTRにAVデータを記録することができる。またEMIが01のno more copyの場合は、認証は成功するが、VTRはno more copyを記録してはいけなないので、EMI情報から

判断してそのAVデータを記録しない。また、本発明のハードディスク装置が2台あって一方がEMIが11のcopy neverのAVデータを出力して（こちらをディスク装置Aとする）、もう一方が前記AVデータを記録する（こちらをディスク装置Bとする）場合が考えられる。この場合、方式Aの認証を互に行い、AVデータはディスク装置Aからディスク装置Bへ転送することができる。このときディスク装置Aは1回しか前記AVデータを出力しないので、ディスク装置Aはこれ以上前記AVデータを出力することができない。結果として前記AVデータはディスク装置Aからディスク装置Bへデータの移動が行われたことになる。しかしながらデータの移動先はテレビモニタではないのでこの間ユーザは前記AVデータを視聴することはできない。つまりAVデータの移動が可能である。このようにして利用許諾を容易に守ることができる。

【0076】さらに前述したように、STB以外の装置から送られてきたAVデータを本発明のハードウェア装置に記録する場合について説明する。STBから送られてきたAVデータはEMIが01のno more copyであるものは存在しなかったが、STB以外の装置から送られてくる場合、EMIがno more copyのAVデータも存在する。EMIが01のno more copyである場合は、データブロックアクセス手段18とEMIアクセス手段11でAVデータとEMI情報をディスク媒体6に記録しないようにする。それ以外はSTBから送られてきたAVデータを記録する場合と同様である。また本発明のハードディスク装置どうして再生記録を行う場合は、EMIが11のcopy neverのAVデータは再生する装置から記録する装置に移動することができる。

【0077】EMIが11以外のときは本発明のハードディスク装置とVTRとを接続した場合と同様の動作となる。このようにEMIに対応して認証の方式を選択することによりcopy neverのようなより重要なAVデータは公開鍵等のより安全な方式を用いて認証することができる。

【0078】ここで、再生情報とAVデータをディスク媒体に格納する例として次の2通りの場合を説明する。

【0079】まずはじめに再生情報をブロック単位に持たせる場合を説明する。図5において、ディスク媒体6は、システム領域31とユーザ領域32に分けられている。システム領域31はシステムが使用する領域で、ユーザがアクセスすることはできない領域である。一方ユーザ領域32はユーザが使用する領域である。ユーザ領域32はk個のブロックから構成されているものとする。システム領域31の一部に再生情報記録部33が設けられている。再生情報記録部33にブロックごとの再生情報を記録する。ブロック1(34)、ブロック2(35)、ブロック3(36)、ブロックk(37)の

再生情報は再生情報記録部(33)のビットマップ形式で保存されたテーブルを参照すると全て0となっている。つまり未再生の領域であることを表す。ただし、ブロックk(37)などの領域はまだ使われていない領域であり、未使用の領域も再生情報としては0としておくものとする。またブロック11、ブロック12、ブロック13の再生情報は1となっているので、再生済みの領域である。このような再生情報記録部31は再生情報管理手段A17で作成、更新される。再生情報記録部33はシステム領域31に格納されているので、容易にユーザが再生情報記録部33の内容を改竄して不正にAVデータを視聴することができないようになっている。従って本実施の形態の機能を有するハードディスクの信頼性を高いものにしている。

【0080】次に再生情報をアドレスで管理する場合を説明する。図6において、ディスク媒体6が、システム領域38とユーザ領域39に分けられている。システム領域38はシステムが使用する領域で、ユーザがアクセスすることはできない領域である。一方ユーザ領域39はユーザが使用する領域である。再生情報が再生済みから未再生あるいは未再生から再生済みに変化することにデータ分割してストリームを定義した。そして再生情報記録部40は、そのストリームの再生情報とそのストリームの開始LBAと終了LBAで再生情報を表すようにした。ストリーム1(41)は、開始LBAが0であり終了LBAがa1であり、このストリームはすべて未再生である。ストリーム2(42)は、開始LBAがa1であり、終了LBAがa2であり、このストリームはすべて再生済みである。ストリーム3(43)は、開始LBAがa2であり、終了LBAがa3であり、このストリームは未再生である。またストリームn(44)は、開始LBAがa4であり、終了LBAがa5であり、このストリームの再生情報は再生済みである。このような再生情報記録部40は再生情報管理手段A17で作成、更新される。再生情報記録部40はシステム領域38に格納されているので、容易にユーザがその内容を改竄して、不正にAVデータを視聴することができないようになっている。従って本実施の形態のハードディスク装置の信頼性を高いものにしている。

【0081】なお再生情報記録部33または40はシステム領域31または38に置く他に、ハードディスク装置の場合交替セクタ領域に置いてよい。

【0082】さらに以上説明した実施の形態においてハードディスク装置を用いる代わりに光ディスク装置(DVD-RAMなど)でも実施可能である。この時再生情報記録部33または40は、光ディスク装置を用いて実施する場合、ユーザが不正にアクセスできない領域として、図24に示すようにDVD-Rの場合ならばレーザーパワーの調整などに使用される試し書きのための領域でパワーキャリブレーションエリア(PCA)と呼ばれ

る領域や、データを追記する場合の追記位置情報などを記録するレコーディングマネージメントエリア(RMA)と呼ばれる領域でもよい。また、TOC情報などが記録されているリードインエリアや終わりを示すリードアウトエリアでもよい。また図25に示すようにDVD-RAMの場合は上記エリアに加えて各セクタ毎のID情報などが記録されているヘッダ部であってもよい。またDVD-RAMにおいても交代セクタ領域に記録してもよい。要するに記録装置の形態にかかわらず、ユーザが直接データを変更できない領域であればどこに再生情報を記録してもよい。

【0083】さらにEMI情報はEMIアクセス手段11によってLBAアクセス手段を介してディスク媒体6に対して記録再生されるが、EMI情報を再生情報と同じようにディスク媒体6のシステム領域等のユーザがデータを直接変更することができない領域に記録することによって、容易にユーザがEMI情報を改竄して、不正にAVデータを視聴することができないようにすることができる。従って本実施の形態のハードディスク装置の信頼性を高いものにすることができる。

【0084】(実施の形態2)次に第2の実施の形態について説明する。

【0085】本実施の形態では、放送局から送られてくるAVデータの利用許諾情報が複製禁止を意味するcopy neverである場合に、放送が行われた時間帯以後の任意の時間にその番組を一回だけ視聴できる記録再生装置の例としてハードディスク装置について説明する。

【0086】本実施の形態では、利用許諾情報がcopy neverであるAVデータを記録可能とし、再生情報管理手段を用いてそのAVデータを一回しか再生できないようにすることでこのようなハードディスク装置を実現した。

【0087】第1の実施の形態では再生情報は、データブロックとは別の領域に記録されていたが、本実施の形態では再生情報をデータブロックとは同じ領域に記録する。

【0088】以下、第1の実施の形態と異なる点について構成を説明する。

【0089】図7において、再生情報管理手段B45は、指定されたデータブロックに対応した再生情報を読み出して更新し、また再生情報から再生済みかどうかを判断する手段である。再生情報生成及びEMI混合手段46は、EMI情報、再生情報をデータブロックと対にし、再生情報は未再生の状態を表すように初期化する手段である。再生情報EMI分離手段47は、対になっているEMI情報、再生情報とデータブロックを分離抽出する手段である。

【0090】また再生情報管理手段B45は以下のように構成される。すなわち、再生情報管理手段B45は、

再生情報更新手段26、再生済判定手段27、再生情報アクセス手段29、切替スイッチ48から構成される。

【0091】再生情報更新手段26は、再生情報を更新する手段で、AVデータが再生済みであるという情報に更新する手段である。例えば再生済みフラグ`play_flag`=1で更新する手段である。再生情報アクセス手段29は、各データブロックに対応する再生情報を更新し、またLBAアクセス手段3を経由してディスク媒体6に記録を行い、また各データブロックに対応する再生情報をテーブルで記憶し、キャッシュする機能を有する手段である。再生済判定手段27は、再生情報アクセス手段29が読み出した再生情報に基づいて、再生済みであるかどうかを判定する手段である。例えば、再生済みフラグが`play_flag`=1ならば1回再生されたと判断し、またEMI判定結果を使ってEMI=11の場合、かつ未再生と判断したら切替スイッチ48を再生情報更新手段26の側に切り替えて、再生情報を更新する手段である。また再生済み判定手段27は、EMI=11でかつ再生済みと判定した場合切替スイッチ19をオフにするか、または無効データ出力手段14に切り替える手段である。

【0092】次に、このような本実施の形態の動作を説明する。

【0093】本実施の形態では、第1の実施の形態と同様STBより送られてくるAVデータをハードディスク装置が記録再生するものとする。STBと本実施の形態のハードディスク装置の認証・鍵交換は第1の実施の形態と同一であるので記述を省略する。

【0094】さて、デジタルI/F手段1を介して、アクセス方式2のコマンドで、記録コマンドを受信したとする。これ以後の処理を図10のフローチャート図を参照して説明する。切替スイッチ24は、送られてくるAVデータのEMIが00でない場合、AVデータが復号化手段20を経由するように切り替える。また切替スイッチ24は、EMIが00の場合、AVデータが復号化手段20を経由しないように切り替える。そして復号化手段20は、受け取った鍵を用いて暗号化されているAVデータを復号化する。ストリームアクセス手段16は、データブロックアクセス手段18にブロックxの記録を指示する。データブロックアクセス手段18は、再生情報管理手段B45に現在アクセス中のブロック番号(=x)を通知する。EMI検出手段9で検出されたEMIは、EMI判定手段12で許諾の有無と種類を判定されたあと、判定結果は再生情報生成及びEMI混合手段46に渡される。再生情報生成及びEMI混合手段46は、EMI情報、再生情報をデータブロックと対にし、再生情報は未再生の状態を表すように初期化する。すなわち再生情報の再生済みフラグを`play_flag`=0とする(S1)。ただしEMIが10すなわち`copy one generation`の場合は、EMI

Iを01すなわち`no more copy`に書き替える。さらに再生情報生成及びEMI混合手段46は、データブロックアクセス手段18にAVデータ、再生情報、EMI情報を対にしたデータを渡す。データブロックアクセス手段18は、LBAアクセス手段8を介して、この対になったデータをディスク媒体6のブロックxに記憶する(S2)。ブロックxに記録するフォーマットについては後述する。次にブロック番号を1だけ増加する。すなわち $x=x+1$ とする(S3)。次にデジタルI/F手段1から別のコマンドの受信があるかどうか判定する(S4)。別のコマンドを受信していれば処理は終了する。そうでない場合は記録コマンドを受信してから処理を別のコマンドの受信があるまで繰り返す。以上がAVデータをディスク媒体6に記録する場合である。

【0095】次にハードディスク装置が、AVデータを再生する場合を説明する。AVデータをテレビモニタに再生する場合を考える。さらにハードディスクに記録されているAVデータはSTBから記録されたものとする。テレビモニタと本実施の形態のハードディスク装置の認証・鍵交換は第1の実施の形態と同一であるので記述を省略する。

【0096】以後の動作は再生情報管理手段B45でいつ再生情報を更新するかで二通りの動作を行うことができる。第1の場合は、再生終了後にまとめて再生情報を更新する場合であり、第2の場合は、再生中にブロックごとに再生情報を更新する場合である。

【0097】まず第1の場合を図10のフローチャート図を参照して説明する。

【0098】ハードディスク装置は、デジタルI/F手段1からアクセス方式2のコマンドで再生コマンドを受信したとする。ストリームアクセス手段16は、データブロックアクセス手段18にブロックxの再生を指示する。データブロックアクセス手段18は、再生情報管理手段B45に、現在アクセス中のブロック番号(=x)を通知する。同時にデータブロックアクセス手段18は、LBAアクセス手段3を介してディスク媒体6からEMI情報と再生情報が対になったAVデータを読み出す(S5)。再生情報EMI分離手段47は、この対になったデータからEMI情報と再生情報を分離する。EMI情報はEMI付与手段10とEMI判定手段12に渡され、また再生情報は再生済判定手段27に渡される。EMI判定手段12は、EMI情報を判定し、その判定結果は、認証・暗号化手段13と、再生済判定手段27に送られる。

【0099】EMI判定結果でEMIが00の場合(S6)は切替スイッチ25が暗号化手段23を経由しない側に切り替えられ、AVデータは暗号化されないで出力される(S8)。またEMIが00でない場合(S6)は切替スイッチ25は暗号化手段23を経由する側に切

り替えられる。切替スイッチ48は、EMI=11の場合のみ再生時には再生情報更新手段26の側にスイッチを切り替える。再生済判定手段27は、読み出されたEMI情報の判定結果を調べる。

【0100】EMIが11のcopy neverの場合、再生済み判定手段27は、AVデータが未再生であるか再生済みであるかを判定する(S7)。EMIが11のcopy neverであってかつ再生済みである場合は、切替スイッチ19が無効データ出力手段14の側に切り替えられブルーバック画面や黒画面などの無効なデータが出力される(S10)。EMIが11のcopy neverであってかつデータが未再生の場合、またはEMIが11でない場合は、切替スイッチ19は認証・暗号化手段13の側に切り替えられ、AVデータは暗号化手段23で暗号化されて、デジタルI/F手段1を介して出力される(S8)。

【0101】次にブロック番号を1だけ増加する。すなわち $x = x + 1$ とする(S9)。次にデジタルI/F手段1から別のコマンドの受信があるかどうか判定する

(S11)。別のコマンドを受信していれば処理は終了する。再生処理が終了したら、再生情報アクセス手段29で再生したブロックの初期値の番号から最終値の番号までの再生情報をアクセスし、再生情報更新手段26で再生済みすなわち $play_flag = 1$ に更新する(S12)。そうでない場合は再生コマンドを受信してからの処理を別のコマンドの受信があるまで繰り返し行う。以上が第1の場合でAVデータを再生する場合である。

【0102】次に第2の場合を図11のフローチャート図を参照して説明する。

【0103】ハードディスク装置は、デジタルI/F手段1からアクセス方式2のコマンドで再生コマンドを受信したとする。ストリームアクセス手段16は、データブロックアクセス手段18にブロックxの再生を指示する。データブロックアクセス手段18は、再生情報アクセス手段29に現在アクセス中のブロック番号(=x)を通知する。同時にデータブロックアクセス手段18は、LBAアクセス手段3を介してディスク媒体6からEMI情報、再生情報と対になったAVデータを読み出す(S17)。再生情報EMI分離手段47は、その対になったAVデータからEMI情報と再生情報を分離する。EMI情報は、EMI付与手段10とEMI判定手段12に渡され、再生情報は、再生済判定手段27に渡される。EMI判定手段12は、EMI情報を判定し、その判定結果は、認証・暗号化手段13と、再生済判定手段27に送られる。

【0104】EMI判定結果でEMIが00の場合(S18)は切替スイッチ25が暗号化手段23を経由しない側に切り替えられ、AVデータは、認証・暗号化手段13を経由しないで、EMI付与手段10でEMI情報

を付与されたあと、デジタルI/F手段1を介して、暗号化されないで出力される(S21)。またEMIが00でない場合(S18)は切替スイッチ25は暗号化手段23を経由する側に切り替えられる。切替スイッチ30は、再生時には再生情報更新手段26の側に切り替える。再生済判定手段27は、読み出されたEMI情報の判定結果を調べる。

【0105】EMIが11のcopy neverの場合、AVデータが未再生であるか再生済みであるかを判定する(S19)。EMIが11のcopy neverであってかつ再生済みすなわち $play_flag = 1$ である場合は、切替スイッチ19が無効データ出力手段14の側に切り替えられブルーバック画面や黒画面などの無効なデータが出力される(S22)。再生済判定手段27で、EMIが11のcopy neverであってかつデータが未再生であるすなわち $play_flag = 0$ と判定された場合、再生情報更新手段26が再生情報をデータが再生済みにすなわち $play_flag = 1$ に更新する(S20)。次に切替スイッチ19は認証・暗号化手段13の側に切り替えられ、データブロックアクセス手段18で読み出されたAVデータは、暗号化手段23で暗号化されて、EMI付与手段10でEMIを付与された後、デジタルI/F手段1を介して出力される(S21)。さらに再生情報アクセス手段29でブロックxの再生情報を更新する(S23)。次にブロックxを $x + 1$ とおき(S24)、再生コマンド以外のコマンドを受信したら(S25)処理を終了する。そうでない場合は再生コマンドを受信してからの処理を別のコマンドの受信があるまで繰り返し行う以上が第2の場合でAVデータを再生する場合である。

【0106】前述したように、再生情報生成及びEMI混合手段46で生成され、再生情報管理手段B45で更新されるデータのフォーマットについて説明する。図9にディスク媒体6のユーザ領域を示す。ユーザ領域はブロック1(49)、ブロック2(50)、ブロック3(51)・・・ブロックk(52)のk個のブロックに分割されている。ブロック1にはEMI53が格納され、その次に再生情報54が格納され、最後にAVデータ55が格納される。再生情報は、再生済みフラグが $play_flag = 0$ のとき未再生であり、 $play_flag = 1$ のとき再生済みである。このようにEMI情報と再生情報とAVデータを対にして同じ領域に格納することによって、一回のディスク媒体へのアクセスで一度に3種類の情報が処理できるので、ディスク媒体へのアクセスのオーバーヘッドが少なくなる。

【0107】以上説明した第2の実施の形態において、再生情報生成及びEMI混合手段46によってAVデータと再生情報を混合し、また再生情報EMI分離手段47によってAVデータと再生情報を分離することによって、再生情報を第1の実施の形態のようにシステム領域

に記録しなくても(ユーザ領域に記録しても)ユーザがデジタルI/F手段1を介して直接再生情報に変更を加えることができないように構成した。従って不正な再生情報の改竄を防ぎ、本実施の形態のハードディスク装置の信頼性を高いものになっている。

【0108】なお第2の実施の形態においてEMI情報は再生情報と別にシステム領域に記録して実施しても構わない。またその逆に第1の実施の形態においてEMI情報のみを第2の実施の形態のようにユーザ領域に記録して、再生情報はシステム領域に記録して実施してもよい。すなわち、再生情報、EMI情報の記録方法は第1の実施の形態及び第2の実施の形態で示した方法のうちの考えられるいずれかの方法で記録してもよい。

【0109】(実施の形態3)次に第3の実施の形態について説明する。

【0110】本実施の形態では、放送局から送られてくるAVデータの利用許諾情報が複製禁止を意味するcopy neverである場合に、放送が行われた時間帯以後の任意の時間にその番組を一回だけ視聴できる記録再生装置の例としてハードディスク装置について説明する。

【0111】本実施の形態では、利用許諾情報がcopy neverであるAVデータを記録可能とし、再生中または再生後にAVデータを消去することによりそのAVデータを一回しか再生できないようにすることでこのようなハードディスク装置を実現した。

【0112】以下、第1の実施の形態と異なる点について構成を説明する。

【0113】本実施の形態の構成を図26に示す。第1の実施の形態で用いた図2の構成において以下の点が異なるのみである。すなわち再生情報管理手段Aと無効データ出力手段を持たない構成にした。また切替スイッチ19は常に暗号化データ出力側に接続されているものとする。またデータブロックアクセス手段はEMI判定手段の判定結果を入力し、結果に応じたアクセスを行うことができるものとする。

【0114】次に、このような本実施の形態の動作を説明する。

【0115】本実施の形態では、第1の実施の形態と同様STBより送られてくるAVデータをハードディスク装置が記録再生するものとする。STBと本実施の形態のハードディスク装置の認証・鍵交換は第1の実施の形態と同一であるので記述を省略する。

【0116】さて、デジタルI/F手段1を介して、アクセス方式2のコマンドで、記録コマンドを受信したとする。これ以後の処理を図22のフローチャート図を参照して説明する。切替スイッチ24は、送られてくるAVデータのEMIが00でない場合、AVデータが復号化手段20を経由するように切り替える。また切替スイッチ24は、EMIが00の場合、AVデータが復号化

手段20を経由しないように切り替える。そして復号化手段20は、受け取った鍵を用いて暗号化されているAVデータを復号化する。ストリームアクセス手段16は、データブロックアクセス手段18にブロックxの記録を指示する。データブロックアクセス手段18は、EMIアクセス手段11に現在アクセス中のブロック番号(=x)を通知する。EMIアクセス手段11は、EMI検出手段9で検出されたEMI情報を、通知されたブロック番号に対応付けて記録する。ただしEMIが10すなわちcopy one generationの場合はディスク媒体6にEMI情報を記録する際にEMIを01すなわちno more copyに書き替えて記録する(S50)。

【0117】次にブロック番号を1だけ増加する。すなわち $x = x + 1$ とする(S51)。次にデジタルI/F手段1から別のコマンドの受信があるかどうか判定する(S52)。別のコマンドを受信していれば処理は終了する。そうでない場合は記録コマンドを受信してからの処理を別のコマンドの受信があるまで繰り返す。以上がAVデータをディスク媒体6に記録する場合である。

【0118】次にハードディスク装置が、AVデータを再生する場合を説明する。AVデータをテレビモニタに再生する場合を考える。さらにハードディスクに記録されているAVデータはSTBから記録されたものとする。テレビモニタと本実施の形態のハードディスク装置の認証・鍵交換は第1の実施の形態と同一であるので記述を省略する。

【0119】以後の動作はいつAVデータを消去するかで二通りの動作を行うことができる。第1の場合は、再生終了後にまとめてAVデータを消去する場合であり、第2の場合は、再生中にブロックごとにAVデータを消去する場合である。

【0120】まず第1の場合を図22のフローチャート図を参照して説明する。

【0121】まず最初に全ブロックの消去フラグ=「偽」で初期化する(S53)。この消去フラグは各ブロックに1対1対応のフラグであり、消去フラグ=「真」であるブロックは後に消去する必要があることを意味するものである。

【0122】ハードディスク装置は、デジタルI/F手段1からアクセス方式2のコマンドで再生コマンドを受信したとする。ストリームアクセス手段16は、データブロックアクセス手段18にブロックxの再生を指示する。データブロックアクセス手段18は、EMIアクセス手段11に、現在アクセス中のブロック番号(=x)を通知する。同時にデータブロックアクセス手段18は、LBAアクセス手段3を介してディスク媒体6からAVデータを読み出す(S54)。EMIアクセス手段11は、通知されたブロック番号に対応するEMI情報

をディスク媒体6から読み出す。読み出されたEMI情報はEMI判定手段12で判定され、その判定結果は、認証・暗号化手段13に送られる。EMI判定結果でEMIが00の場合(S55)は切替スイッチ25が暗号化手段23を経由しない側に切り替えられ、AVデータは暗号化されないで出力される(S57)。またEMIが00でない場合(S55)は切替スイッチ25は暗号化手段23を経由する側に切り替えられる。

【0123】EMIが11の場合はブロック番号に対応する消去フラグを「真」に書き替える。次にEMIが00でない場合、切替スイッチ19は認証・暗号化手段13の側に切り替えられ、AVデータは暗号化手段23で暗号化されて、デジタルI/F手段1を介して出力される(S57)。

【0124】次にブロック番号を1だけ増加する。すなわち $x = x + 1$ とする(S58)。次にデジタルI/F手段1から別のコマンドの受信があるかどうか判定する(S59)。別のコマンドを受信していれば処理は終了する。再生処理が終了したら、再生したブロックの初期値の番号から最終値の番号までのうち、消去フラグ＝「真」のブロックについて、AVデータを消去するか、ブロックxのディスク上の記録位置へのリンク情報を消去する(S60)。そうでない場合は再生コマンドを受信してから処理を別のコマンドの受信があるまで繰り返し行う。以上が第1の場合でAVデータを再生する場合である。

【0125】次に第2の場合を図23のフローチャート図を参照して説明する。

【0126】ハードディスク装置は、デジタルI/F手段1からアクセス方式2のコマンドで再生コマンドを受信したとする。ストリームアクセス手段16は、データブロックアクセス手段18にブロックxの再生を指示する。データブロックアクセス手段18は、EMIアクセス手段11に現在アクセス中のブロック番号(=x)を通知する。同時にデータブロックアクセス手段18は、LBAアクセス手段3を介してディスク媒体6からAVデータを読み出す(S64)。EMIアクセス手段11は、通知されたブロック番号に対応するEMI情報をディスク媒体6から読み出す。読み出されたEMI情報はEMI判定手段12で判定され、その判定結果は、認証・暗号化手段13と、再生済判定手段27に送られる。

【0127】EMI判定結果でEMIが00の場合(S66)は切替スイッチ25が暗号化手段23を経由しない側に切り替えられ、AVデータは、認証・暗号化手段13を経由し、デジタルI/F手段1を経由して、暗号化されないで出力される。またEMIが00でない場合(S66)は切替スイッチ25は暗号化手段23を経由する側に切り替えられる。次に切替スイッチ19は認証・暗号化手段13の側に切り替えられ、データブロックアクセス手段18で読み出されたAVデータは、暗号化

手段23で暗号化されて、デジタルI/F手段1を介して出力される。ブロックxのEMIが11のときデータブロックアクセス手段18は、ブロックxを消去するかまたは無効なデータを書き込むかまたはブロックxのディスク上の記録位置へのリンク情報を消去する(S67)。次にブロックxを $x + 1$ とおき(S68)、再生コマンド以外のコマンドを受信したら(S69)処理を終了する。そうでない場合は再生コマンドを受信してから処理を別のコマンドの受信があるまで繰り返し行う。

【0128】以上が第2の場合でAVデータを再生する場合である。

【0129】ハードディスクに記録されたAVデータのEMIが11すなわちcopy neverである場合に、AVデータ出力後にそのAVデータのデータブロックを消去するか無効なデータを書き込むかまたはディスク上の記録位置へのリンク情報を消去することにより、copy neverのAVデータを一回だけ再生することができる。

【0130】なお、本実施の形態では、アクセス方式2によってストリームアクセス手段16でコマンドを実行する場合を説明したが、これに限らずアクセス方式3によってファイルアクセス手段15でコマンドを実行してもよい。この場合、記録再生の順序はブロック番号の順序ではなく、ファイル管理情報によって管理するブロックの順序に依存する。つまりx番目に記録再生するブロックを $f(x)$ とすると、図22、図23のブロックxの記述部分はブロック $f(x)$ で置き換えさえすればよい。またブロックxの消去はファイル管理上で消去を行えばよい。

【0131】なお本実施の形態においてEMIは第2の実施の形態のようにAVデータと混合して記録しても同様に実施可能である。

【0132】(実施の形態4)次に第4の実施の形態について説明する。

【0133】本実施の形態では、放送局から送られてくるAVデータの利用許諾情報が複製禁止を意味するcopy neverである場合に、放送が行われた時間帯以後の任意の時間にその番組を一回だけ視聴できる記録再生装置の例としてVCR(ビデオカセットレコーダ)について説明する。

【0134】本実施の形態では、利用許諾情報がcopy neverであるAVデータを記録可能とし、再生情報管理手段を用いてそのAVデータを一回しか再生できないようにすることでこのようなVCRを実現した。

【0135】図12にVCRの基本構成図を示す。VCRはデジタルI/F1、ストリームコントロール手段90、メモリアクセス手段56、記録再生手段57、コントロール手段58、ヘッド60、メモリ59、テープ媒体61より構成される。

【0136】デジタルI/F手段1は第1の実施の形態で説明したものと同一である。ストリームコントロール手段90は、第1の実施の形態で説明したものととの相違点に限って、後述する。メモリアクセス手段56は、テープ媒体61に設けられたメモリ59に対して、EMI情報や再生情報などを記録再生する手段である。記録再生手段57は、ヘッド60からの再生信号を信号処理してデジタルAVデータを出力し、またストリームコントロール手段90から送られてくるAVデータを信号処理してヘッド60に記録信号を送る手段である。コントロール手段58は、テープ媒体61の走行制御、ヘッド60のトラッキング、記録再生手段57のコントロールを行う。ヘッド60はテープ媒体61に信号を記録するかまたはテープ媒体61の信号を再生する。メモリ59は、テープ媒体61に内蔵され、EMI情報や再生情報などを記録再生するものである。

【0137】前述したように図13を参照して、ストリームコントロール手段90の第1の実施の形態との相違点を説明する。コマンド実行手段62は、デジタルI/F手段1から受信されるコマンドを実行する手段である。すなわちコマンドの処理内容を解釈して、再生、記録、停止などをコントロール手段58に指示する手段である。このようなデジタルI/F手段1に送られるコマンドには、AV/C digital Interface Command Set VCR subunit Specification version 2.0.1に準拠した方式などがある。また第1の実施の形態でデータブロックアクセス手段18に代わるものとして、記録再生手段57がある。記録再生手段57は、現在記録または再生中のトラック番号を再生情報管理手段Aに通知する手段である。

【0138】本実施の形態の動作は、第1の実施の形態の動作で「ブロック」を「トラック」におきかえ、さらにファイルアクセス手段15とストリームアクセス手段16をコマンド実行手段62におきかえると、第1の実施の形態の動作と同一になる。このようにして、放送局から送られてくるAVデータの利用許諾情報が複製禁止を意味するcopy neverである場合に、放送が行われた時間帯以後の任意の時間にその番組を一回だけ視聴できるVCRが実現できた。

【0139】ここで、再生情報とAVデータをテープ媒体61に格納する例として次の2通りの場合を説明する。

【0140】まずはじめに再生情報をトラック単位に持たせる場合を説明する。図14において、テープ媒体61は、k個のトラックから構成されている。テープ媒体61にはメモリ59が組み込まれており、メモリ59に再生情報記録部67が記録されている。トラック1(63)、トラック2(64)、トラック3(65)、トラックk(66)の再生情報は、再生情報記録部67にピ

ットマップ形式で保存されたテーブルを参照すると全て0となっている。つまり未再生の領域であることを表す。ただし、トラックk(66)などの領域はまだ使われていない領域であり、未使用の領域も再生情報としては0としておくものとする。またトラック11、トラック12、トラック13の再生情報は1となっているので、再生済みの領域である。このような再生情報記録部67は再生情報管理手段A17で作成、更新される。再生情報記録部67はテープ媒体61に内蔵されているメモリ59に格納されているので、容易にユーザが再生情報記録部67の内容を改竄して不正にAVデータを視聴することができないようになっている。従って本実施の形態のVCRの信頼性を高いものにしている。

【0141】次に再生情報をアドレスで管理する場合を説明する。図15において、テープ媒体61のテープ全体73の部分に、再生情報が再生済みから未再生あるいは未再生から再生済みに変化することにデータを分割してストリームを定義した。そして再生情報記録部67は、そのストリームの再生情報とそのストリームの開始トラックと終了トラックの対で表すようにした。ストリーム1(69)は、開始トラックが0であり終了トラックがa1であり、このストリームはすべて未再生である。ストリーム2(70)は、開始トラックがa1であり、終了トラックがa2であり、このストリームはすべて再生済みである。ストリーム3(71)は、開始トラックがa2であり、終了トラックがa3であり、このストリームは未再生である。またストリームn(72)は、開始トラックがa4であり、終了トラックがa5であり、このストリームの再生情報は再生済みである。このような再生情報記録部67は再生情報管理手段A17で作成、更新される。再生情報記録部67はテープ媒体61のメモリ59に格納されているので、容易にユーザが再生情報記録部67の内容を改竄して、不正にAVデータを視聴することができないようになっている。従って本実施の形態のVCRの信頼性を高いものにしている。

【0142】(実施の形態5)次に第5の実施の形態について説明する。

【0143】本実施の形態では、放送局から送られてくるAVデータの利用許諾情報が複製禁止を意味するcopy neverである場合に、放送が行われた時間帯以後の任意の時間にその番組を一回だけ視聴できる記録再生装置の例としてVCRについて説明する。本実施の形態では、第4の実施の形態とは異なり、EMI情報をAVデータと対してテープに格納した。また利用許諾情報がcopy neverであるAVデータを記録可能とし、再生しながらAVデータを消去することでこのようなVCRを実現した。

【0144】図16にVCRの基本構成図を示す。図12に示したように第4の実施の形態のVCRとの相違点

は第4の実施の形態が記録再生手段であったのを、本実施の形態では再生手段と記録手段を別々の構成にし、ヘッドは記録用ヘッドと再生用ヘッドが別々に設けられ、分離手段と混合手段を設けた点である。VCRはデジタルI/F1、ストリームコントロール手段91、分離手段77、再生手段78、混合手段79、記録手段80、コントロール手段81、ヘッド74、記録用ヘッド75、再生用ヘッド76、テープ媒体61から構成される。

【0145】デジタルI/F手段1は第1の実施の形態で説明したものと同一である。ストリームコントロール手段91の構成は第4の実施の形態と相違する点のみ後述する。分離手段77は、再生手段78から読み出されたデータをEMI情報とAVデータに分離する手段である。混合手段79は、EMI情報とAVデータを対にする手段である。再生手段78は、テープ媒体61に記録されているEMI情報とAVデータをヘッド74の再生用ヘッド76を介して再生する手段である。記録手段80は、ヘッド74の記録用ヘッド75を介してテープ媒体61にEMI情報とAVデータを記録する手段である。ヘッド74は、記録用ヘッド75と再生用ヘッド76から構成され、再生用ヘッド76によりテープ媒体61に記録されている信号を再生し、また記録用ヘッド75でテープ媒体61に信号を記録する手段である。コントロール手段81は、テープ媒体61の走行制御、ヘッド74のトラッキング、再生手段78と記録手段80のコントロールを行う手段である。テープ媒体61は信号を記録するものである。

【0146】前述したようにストリームコントロール手段91の第4の実施の形態との相違点は以下のようになる。切替スイッチ82は、記録中は認証・暗号化手段13からの出力データをそのまま混合手段79に出力するよう切り替え、再生中はEMI判定手段12の判定結果がEMI=11の場合無効データ出力手段14に切り替えるものである。再生中でありかつEMI=01または10の場合は認証・暗号化手段13とも無効データ出力手段14ともつながらないものである。コマンド実行手段62は、第4の実施の形態で記述している内容に加え、切替スイッチ82に記録中か再生中かを通知する手段である。また再生情報管理手段Aは本実施の形態では使われていない。

【0147】次に、このような本実施の形態の動作を説明する。

【0148】本実施の形態では、第1の実施の形態と同様STBより送られてくるAVデータをVCRが記録再生するものとする。STBと本実施の形態のVCRの認証・鍵交換は第1の実施の形態と同一であるので記述を省略する。

【0149】さて、デジタルI/F手段1を介して、コマンド実行手段62が記録コマンドを受信したとする。

コマンド実行手段62は、記録コマンドを受信したことを切替スイッチ82に通知する。すると切替スイッチ82は、送られてくるAVデータが認証・暗号化手段13から混合手段79へ渡されるように切り替える。送られてくるAVデータのEMIが00でない場合、AVデータが復号化手段20を経由するように切替スイッチ24を切り替える。またEMIが00の場合、AVデータが復号化手段20を経由しないように切替スイッチ24を切り替える。そして復号化手段20は、STBから受け取った鍵を用いて暗号化されているAVデータを復号化する。混合手段79は、EMI検出手段9で検出されたEMI情報を受け取り、また認証・暗号化手段13から出力されるAVデータを切替スイッチ82を介して受け取る。混合手段79は受け取ったEMI情報とAVデータを対にする。そうして、記録手段80は、対になったAVデータとEMI情報をヘッド74の記録用ヘッド75を介して、テープ媒体61に記録する。ただしEMI情報は、EMIが10すなわちcopy one generationの場合はディスク媒体6にEMI情報を記録する際にEMIを01すなわちnomore copyに書き替えて記録する。AVデータとEMI情報がテープ媒体61に記録されるフォーマットについては後述する。このような処理を別のコマンドの受信があるまで続ける。以上がテープ媒体61に記録する場合の処理である。

【0150】次にVCRがAVデータを再生する場合を説明する。AVデータをテレビモニタに再生する場合について説明する。さらにVCRに記録されているAVデータはSTBから記録されたものとする。テレビモニタと本実施の形態のVCRの認証・鍵交換は第1の実施の形態と同一であるので記述を省略する。

【0151】VCRは、デジタルI/F手段1から再生コマンドを受信したとする。そうすると、コマンド実行手段62は切替スイッチ82に再生コマンドを受信したことを通知する。そうすると切替スイッチ82はEMI判定手段12の判定結果が11の場合、無効データ出力手段82の側に切り替える。またEMI=10または01の場合、切替スイッチ82は認証・暗号化手段13にも無効データ出力手段14にもつながらない。ただし、本実施の形態の場合STBから記録されたAVデータを再生する場合を扱っているので、EMI=10のAVデータは存在しない。すなわちSTBから記録されるときはAVデータのEMIで10のものはすべて01に書き替えられている。分離手段77は、テープ媒体61からヘッド74、再生手段78を介して再生されたAVデータとEMI情報を分離する。AVデータは認証・暗号化手段13に渡される。またEMI情報はEMI付与手段10に渡され、認証・暗号化手段13を介して出てきたAVデータもEMI付与手段10を経由し、ここでAVデータはEMIを付与されたあとデジタルI/F手段1を

介して出力される。分離手段77がAVデータとEMI情報を分離する直後に、混合手段79は、EMIが11のとき、無効データ出力手段14により無効データを、記録手段80、ヘッド74の記録用ヘッド75を介してテープ媒体61に書き込む。このようにして再生されたテープ媒体61上のAVデータは、ブルーバック画面や黒画面などの無効データで書き替えられてしまう。このようにして、放送局から送られてくるAVデータの利用許諾情報が複製禁止を意味するcopy neverである場合に、放送が行われた時間帯以後の任意の時間にその番組を一回だけ視聴できるVCRが実現できた。

【0152】前述したように、AVデータとEMI情報がテープ媒体61に記録されるフォーマットについて説明する。

【0153】図18に示すように、テープ84は、トラック単位で記録してゆき、記録されたトラックにはトラック番号84が付される。一つのトラックは、EMI情報記録部85とデータ記録部86の2つの領域に分割される。EMI情報記録部85は、EMI情報を記録する。またデータ記録部86はAVデータを記録する。

【0154】なお、本発明のEMI情報は上述した実施の形態におけるEMI情報記録部に記録されるものに限らない。テープ媒体にメモリを搭載してメモリに記録してもよい。このようにすることによって情報が改竄できにくくなりシステムの信頼性が向上する。

【0155】(実施の形態6)次に第6の実施の形態について説明する。

【0156】本実施の形態では、放送局から送られてくるAVデータの利用許諾情報が複製禁止を意味するcopy neverである場合に、放送が行われた時間帯以後の任意の時間にその番組を一回だけ視聴できる記録再生装置の例としてハードディスク装置について説明する。本実施の形態では、利用許諾情報がcopy neverであるAVデータを記録可能とし、AVデータを第2暗号/復号化手段により再暗号化して記録し、再生時に第2暗号/復号化手段で用いる鍵を消去しながら再生することによってこのようなハードディスク装置を実現した。

【0157】図1は本発明のハードディスク装置の基本構成図である。これについては第1の実施の形態で説明したのと同じである。図1でハードディスク装置のストリームコントロール手段2は、図19のように構成される。すなわちストリームコントロール手段2は、EMI検出手段9、EMI付与手段10、EMIアクセス手段11、EMI判定手段12、認証・暗号化手段13、ファイルアクセス手段15、ストリームアクセス手段16、データブロックアクセス手段18、時変鍵手段87、鍵アクセス手段88、第2暗号/復号化手段89から構成される。

【0158】ストリームコントロール手段2の構成のう

ち、第1の実施の形態と相違している部分のみ説明する。時変鍵手段87は、時間とともにランダムに変化する鍵を生成する手段であり、生成された鍵は鍵アクセス手段88と第2暗号/復号化手段89に渡される手段である。鍵アクセス手段88は、時変鍵生成手段87で生成された鍵を、対応するデータブロックと関連づけて記憶し、ディスク媒体6に記録し、ディスク媒体6から読み出す手段である。第2の暗号/復号化手段89は、入力された鍵をもとにAVデータを暗号化または復号化する手段である。

【0159】次にこのような本実施の形態の動作について説明する。

【0160】本実施の形態では、第1の実施の形態と同様記録時にはSTBより送られてくるAVデータをハードディスク装置が記録再生するものとする。STBと本実施の形態のハードディスク装置の認証・鍵交換は第1の実施の形態と同一であるので記述を省略する。

【0161】デジタルI/F手段1を介して、アクセス方式2のコマンドで、記録コマンドを受信したとする。これ以後の処理を図20のフローチャート図を参照して説明する。デジタルI/F手段1を介して、切替スイッチ24は、送られてくるAVデータのEMIが00でない場合、AVデータが復号化手段20を経由するように切り替える。またEMIが00の場合、AVデータが復号化手段20を経由しないように切り替える。そして復号化手段20は、受け取った鍵を用いて暗号化されているAVデータを復号化する。ストリームアクセス手段16は、データブロックアクセス手段18にブロックxの記録を指示する。データブロックアクセス手段18は、EMIアクセス手段11に現在アクセス中のブロック番号(=x)を通知する。EMIアクセス手段11は、EMI検出手段9で検出されたEMI情報を、通知されたブロック番号に対応付けて記録する。ただしEMIが10すなわちcopy one generationの場合はディスク媒体6にEMI情報を記録する際にEMIを01すなわちno more copyに書き替えて記録する。また時変鍵手段87で鍵を生成する。生成された鍵は鍵アクセス手段88に渡され、LBAアクセス手段3を介してディスク媒体6に記録される(S26)。またこの鍵は第2暗号/復号化手段89に渡され、認証・暗号化手段13から受け取ったAVデータを再び暗号化し、暗号化されたAVデータはデータブロックアクセス手段18に渡され、LBAアクセス手段3を介して、ディスク媒体6に記録される(S27)。次にブロック番号を1だけ増加する。すなわち $x = x + 1$ とする(S28)。次にデジタルI/F手段1から別のコマンドの受信があるかどうか判定する(S29)。別のコマンドを受信していれば処理は終了する。そうでない場合は記録コマンドを受信してから処理を別のコマンドの受信があるまで繰り返し行う。以上がAVデータを

ディスク媒体6に記録する場合である。

【0162】次にハードディスク装置が、AVデータを再生する場合を説明する。AVデータをテレビモニタに再生する場合を考える。さらにハードディスクに記録されているAVデータはSTBから記録されたものとする。テレビモニタと本実施の形態のハードディスク装置の認証・鍵交換は第1の実施の形態と同一であるので記述を省略する。

【0163】再生時の動作は時変鍵生成手段87で生成された鍵をディスク媒体6からいつ消去するかで二通りの動作を行うことができる。第1の場合は、再生終了後にまとめて鍵を消去する場合であり、第2の場合は、再生中にブロックごとに鍵を消去する場合である。

【0164】まず第1の場合を図20のフローチャート図を参照して説明する。

【0165】ハードディスク装置は、デジタルI/F手段1からアクセス方式2のコマンドで再生コマンドを受信したとする。ストリームアクセス手段16は、データブロックアクセス手段18にブロックxの再生を指示する。データブロックアクセス手段18は、EMIアクセス手段11と鍵アクセス手段88に、現在アクセス中のブロック番号(=x)を通知する。同時にデータブロックアクセス手段18は、LBAアクセス手段3を介してディスク媒体6からAVデータを読み出す(S30)。EMIアクセス手段11は、通知されたブロック番号に対応するEMI情報をディスク媒体6から読み出す。読み出されたEMI情報はEMI判定手段12で判定され、その判定結果は、認証・暗号化手段13と、鍵アクセス手段88に送られる。鍵アクセス手段88は、ブロックxの鍵をディスク媒体6から読み出す(S31)。さらに鍵アクセス手段88は、読み出した鍵を第2暗号/復号化手段89に渡し、第2暗号/復号化手段89は、データブロックアクセス手段18より受け取ったブロックxのAVデータを復号化する(32)。さらに鍵アクセス手段88は、ブロックxの鍵の消去フラグを0にセットする(S33)。EMI判定結果でEMIが00の場合(S34)は、切替スイッチ25が暗号化手段23を経由しない側に切り替えられ、AVデータは暗号化されないで出力される。またEMIが00でない場合(S34)は切替スイッチ25は暗号化手段23を経由する側に切り替えられる。

【0166】EMIが11すなわちcopy neverである場合、またはEMIが01すなわちno more copyの場合、第2暗号/復号化手段89は、復号化したブロックxのAVデータを、認証・暗号化手段13に渡す。

【0167】その後、鍵アクセス手段88は、ブロックxの鍵の消去フラグを1に設定する(S35)。次にブロック番号を1だけ増加する。すなわち $x = x + 1$ とする(S36)。次にデジタルI/F手段1から別のコマ

ンドの受信があるかどうか判定する(S37)。別のコマンドを受信していれば処理は終了する。再生処理が終了したら、鍵アクセス手段は、EMIが11の場合に限り、ブロックの初期値の番号から最終値の番号までの消去フラグが1のブロックの鍵を消去する(S38)。消去するとは、例えば無効なデータで鍵の記録部分を上書きするとか、または鍵が記録されているディスク媒体上の記録位置へのリンク情報を消去してもよい。

【0168】次に第2の場合を図21のフローチャート図を参照して説明する。

【0169】ハードディスク装置は、デジタルI/F手段1からアクセス方式2のコマンドで再生コマンドを受信したとする。ストリームアクセス手段16は、データブロックアクセス手段18にブロックxの再生を指示する。データブロックアクセス手段18は、EMIアクセス手段11と鍵アクセス手段88に、現在アクセス中のブロック番号(=x)を通知する。同時にデータブロックアクセス手段18は、LBAアクセス手段3を介してディスク媒体6からAVデータを読み出す(S43)。EMIアクセス手段11は、通知されたブロック番号に対応するEMI情報をディスク媒体6から読み出す。読み出されたEMI情報はEMI判定手段12で判定され、その判定結果は、認証・暗号化手段13と、鍵アクセス手段88に送られる。鍵アクセス手段88は、ブロックxの鍵をディスク媒体6から読み出す(S44)。さらに鍵アクセス手段88は、読み出した鍵を第2暗号/復号化手段89に渡し、第2暗号/復号化手段89は、データブロックアクセス手段18より受け取ったブロックxのAVデータを復号化する(S45)。EMI判定結果でEMIが00の場合(S46)は、切替スイッチ25が暗号化手段23を経由しない側に切り替えられ、AVデータは暗号化されないで出力される。またEMIが00でない場合(S46)は切替スイッチ25は暗号化手段23を経由する側に切り替えられる。

【0170】EMIが11すなわちno more copyの場合、第2暗号/復号化手段89は、復号化したブロックxのAVデータを、認証・暗号化手段13に渡す。その後、鍵アクセス手段88は、ブロックxの鍵を消去する(S47)。消去するとは、無効なデータで鍵の記録部分を上書きするか、または鍵が記録されているディスク媒体上の記録位置へのリンク情報を消去してもよい。

【0171】EMIが01すなわちno more copyである場合、第2暗号/復号化手段89は、復号化したブロックxのAVデータを出力する。この場合はブロックxの鍵を消去しない(S47)。

【0172】次にブロック番号を1だけ増加する。すなわち $x = x + 1$ とする(S48)。次にデジタルI/F手段1から別のコマンドの受信があるかどうか判定する(S49)。別のコマンドを受信していれば処理は終了

する。

【0173】このように、本実施の形態では、AVデータを暗号化してメディアに記録するため、暗号化されていないAVデータを記録するよりもDVD-RAMなどの交換可能なメディアの場合、不正使用に対して安全性を高めることができる。

【0174】なお本実施の形態における鍵の記録方法はAVデータと対にして記録してもよいし、AVデータとは別々に記録してもよい。その際、鍵はユーザが直接アクセスできない領域すなわちシステム領域などに記録してもよい。またユーザが直接アクセスできない領域とはこれに限らず第1の実施の形態で説明したように交代セクタ領域、PCA、RMA、リードイン、リードアウトまたはDVD-RAM媒体上のヘッダ部であってもよい。要するにユーザが直接アクセスできない領域であればなんでもよい。このようにすれば鍵のデータをユーザがアクセスすることによって解読されるおそれなくなりより安全性が向上するものである。

【0175】さらに本実施の形態では再生時に鍵を消去することで1回だけ再生できる方法を説明したが、鍵に対しての再生情報を管理しても同様に実施可能である。すなわち鍵に対して読み出し済であるか否かを鍵の再生情報として、第1または第2の実施の形態で説明した再生情報と同様に管理して実施することにより、鍵を1回しか読み出すことが出来なくなり、結果として再生時には1回だけ記録媒体上に暗号化されて記録されているAVデータを再生することができるものである。

【0176】さらに鍵の再生情報も上述したようにユーザがアクセスできない領域に記録するとより安全性が向上する。

【0177】さらに第1から第6の実施の形態において、EMI=11のcopy neverのAVデータについて、1回だけ再生できる装置について説明したが、EMI=10のcopy one generationのAVデータをEMI=01のno more copyにして記録されている場合に、前記AVデータをEMI=10のcopy one generationで1回だけ再生することによって、機器間で前記AVデータの移動を行うことが可能である。この場合AVデータの移動を要求するコマンドに対して、EMI=01で記録されたAVデータをEMI=10にして出力する以外は第1から第6の実施の形態と同様にして実施可能である。EMI=11のAVデータの移動については第1の実施の形態ですでに説明しているが、このようにしてEMI=11以外のAVデータについても移動が可能となる。これによりユーザはAVデータを保存する媒体を自由に選択できるという利点がある。

【0178】さらに第1から第6の実施の形態ではEMIを用いたが、EMIに限らず、CGMSを用いて許諾の有無と種別を判定してもよい。CGMSを用いて許諾

の有無と種別を判定する場合は、CGMSを検出するために本発明の記録再生装置にトランスポートデコーダが必要になり、装置構成が複雑になるが、EMIを用いる場合と同等の効果がある。CGMSの場合、copy one generationのまま1回複製されたAVデータを再びcopy one generationのまま出力して1回だけ再生すればよい。

【0179】さらに本発明の無効なデータは本実施の形態におけるブルーバック画面や黒画面に限らず、テストパターン、白画面、視聴できないことを示すメッセージが書かれた画面など、要するに再生対象となっているAVデータ以外のデータでありさえすればよい。

【0180】さらに本発明の時変鍵生成手段は本実施の形態におけるブロックごとに鍵を生成する手段に限らず、2ブロック毎、4ブロック毎に鍵を生成するなど、要するに時間とともに変化する鍵を生成する手段でありさえすればよい。

【0181】さらに本実施の形態のハードディスク装置は本発明の記録再生装置の例であり、本実施の形態のVCRも本発明の記録再生装置の例であり、本実施の形態の再生情報管理手段、EMIアクセス手段、データブロックアクセス手段は本発明の記録手段の例であり、本実施の形態のEMIアクセス手段、再生情報管理手段、データブロックアクセス手段、切替スイッチは本発明の再生手段の例である。

【0182】さらに本発明の記録再生装置は、本実施の形態におけるハードディスク装置やVCRに限らず、光ディスク装置、DVD-RAM装置など、要するに記録再生ができる装置でありさえすればよい。

【0183】さらに第1から第6の実施の形態において説明したLBAアクセス手段は、ハードディスク装置の場合ならばヘッド、シリンダ、セクタによるアクセス手段であってもよい。また光ディスク装置の場合ならば分、秒、フレーム（1フレームは75分の1秒）によるアクセス手段であってもよい。要するにディスク媒体上への物理的なアクセスが可能な手段であれば何でもよい。

【0184】さらに第1から第6の実施の形態において、再生情報が再生みであるAVデータについてデータを出力する相手の機器に対して、無効なデータを出力する代わりに認証において失敗させるかまたはAVデータの復号化の鍵を渡さないように実施してもよい。

【0185】さらに本発明の記録再生装置の各機能の全部または一部の機能をコンピュータに実行させるためのプログラムを格納していることを特徴とするプログラム記録媒体も本発明に属する。

【0186】

【発明の効果】以上説明したところから明らかなように、本発明は番組の利用許諾情報を表す情報が複製禁止の場合に、一回だけ視聴を許可するという著作者の意図

通りにAVデータを視聴者が視聴でき、かつAVデータが放送された時刻以後で時間帯を限定されずにそのAVデータを視聴者が視聴できる記録再生装置及びプログラム記録媒体を提供することができる。また利用許諾情報が複製禁止または1世代のみ複製許可の場合に2回だけ再生することによりAVデータの移動ができ、ユーザは保存する媒体を自由に選択出来る記録再生装置も提供することが出来る。

【図面の簡単な説明】

【図1】本発明の第1、2、3、6の実施の形態におけるハードディスク装置の基本構成図。

【図2】本発明の第1の実施の形態における再生情報とデータブロックとをディスク媒体の別々の領域に記録する場合のストリームコントロール手段の構成を示すブロック図。

【図3】本発明の第1～6の実施の形態における認証・暗号化手段の構成を示すブロック図。

【図4】本発明の第1、4の実施の形態における再生情報管理手段Aの構成を示すブロック図。

【図5】本発明の第1の実施の形態における再生情報とデータブロックとをディスク媒体の別々の領域に記録する場合において再生情報をデータブロック単位でシステム領域に記録する記録方法を示す図。

【図6】本発明の第1の実施の形態における再生情報とデータブロックとをディスク媒体の別々の領域に記録する場合において再生情報が変化する開始LBAと終了LBAとで再生情報を記録する記録方法を示す図。

【図7】本発明の第2の実施の形態における再生情報とデータブロックとをディスク媒体の同じ領域に記録する場合のストリームコントロール手段の構成を示すブロック図。

【図8】本発明の第2の実施の形態における再生情報とデータブロックとをディスク媒体の同じ領域に記録する場合の再生情報管理手段Bの構成を示すブロック図。

【図9】本発明の第2の実施の形態における再生情報とデータブロックとをディスク媒体の同じ領域に記録する場合において再生情報とデータブロックとを記録する記録方法を示す図。

【図10】本発明の第1、2の実施の形態におけるAVデータの記録時と再生時の処理の流れを示し、再生時には再生情報を再生終了後に更新する場合の処理の流れを示すフローチャート図。

【図11】本発明の第1、2の実施の形態におけるAVデータの記録時と再生時の処理の流れを示し、再生時には再生情報を再生中に更新する場合の処理の流れを示すフローチャート図。

【図12】本発明の第4の実施の形態におけるVCRの基本構成図。

【図13】本発明の第4の実施の形態における再生情報をメモリに記録しAVデータをテープに記録する場合の

ストリームコントロール手段の構成を示すブロック図。

【図14】本発明の第4の実施の形態における再生情報をメモリに記録しAVデータをテープに記録する場合において、再生情報をトラック単位で記録する記録方法を示す図。

【図15】本発明の第4の実施の形態における再生情報をメモリに記録しAVデータをテープに記録する場合において、再生情報が変化する開始トラックと終了トラックとで再生情報を記録する記録方法を示す図。

【図16】本発明の第5の実施の形態におけるVCRの基本構成図。

【図17】本発明の第5の実施の形態におけるAVデータを再生しながら消去する場合のストリームコントロール手段の構成を示すブロック図。

【図18】本発明の第5の実施の形態におけるAVデータを再生しながら消去する場合において、EMI情報とAVデータをテープに記録する記録方法を示す図。

【図19】本発明の第6の実施の形態におけるAVデータをディスク媒体に記録する際に再暗号化して記録し、再生する際にAVデータを復号化して出力したあとディスク媒体に記録されている鍵を消去する場合のストリームコントロール手段の構成を示すブロック図。

【図20】本発明の第6の実施の形態におけるAVデータの再生終了後に鍵を消去する場合の処理の流れを示すフローチャート図。

【図21】本発明の第6の実施の形態におけるAVデータの再生中に鍵を消去する場合の処理の流れを示すフローチャート図。

【図22】本発明の第3の実施の形態におけるAVデータの再生後にAVデータを消去する場合の処理の流れを示すフローチャート図。

【図23】本発明の第3の実施の形態におけるAVデータを再生中にAVデータを消去する場合の処理の流れを示すフローチャート図。

【図24】本発明の第1の実施の形態におけるDVD-Rの記録方法を示す図。

【図25】本発明の第1の実施の形態におけるDVD-RAMの記録方法を示す図。

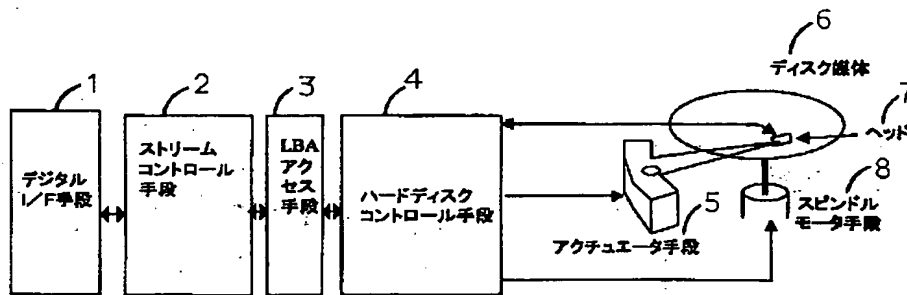
【図26】本発明の第3の実施の形態におけるAVデータの再生中または再生後にAVデータを消去する場合のストリームコントロール手段の構成を示すブロック図。

【符号の説明】

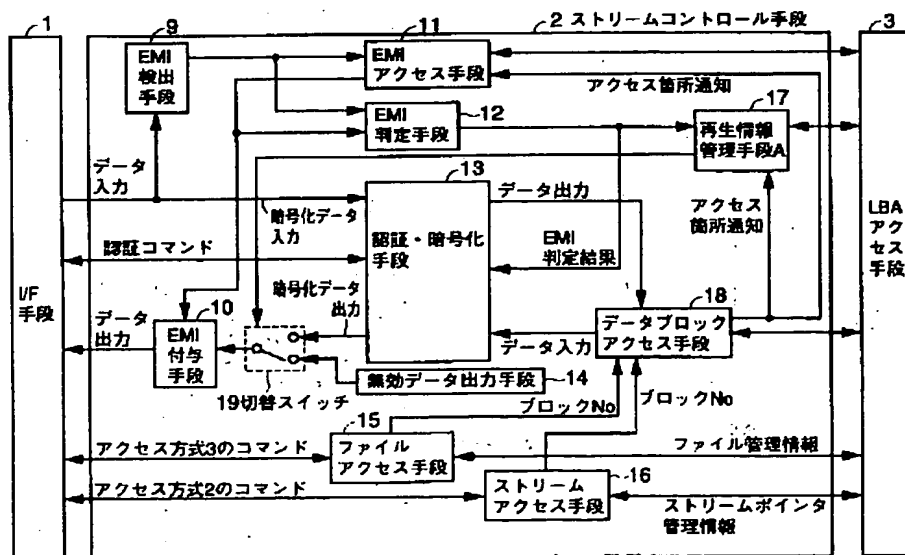
- 1 デジタルI/F手段
- 2 ストリームコントロール手段
- 3 LBAアクセス手段
- 4 ハードディスクコントロール手段
- 5 アクチュエータ手段
- 6 ディスク媒体
- 7 ヘッド
- 8 スピンドルモータ手段

- | | |
|------------------|---------------|
| 9 EMI検出手段 | 20 復号化手段 |
| 10 EMI付与手段 | 21 認証手段 |
| 11 EMIアクセス手段 | 22 鍵生成手段 |
| 12 EMI判定手段 | 23 暗号化手段 |
| 13 認証・暗号化手段 | 24 切替スイッチ |
| 14 無効データ出力手段 | 25 切替スイッチ |
| 15 ファイルアクセス手段 | 26 再生情報更新手段 |
| 16 ストリームアクセス手段 | 27 再生済判定手段 |
| 17 再生情報管理手段A | 28 再生情報生成手段 |
| 18 データブロックアクセス手段 | 29 再生情報アクセス手段 |
| 19 切替スイッチ | 30 切替スイッチ |

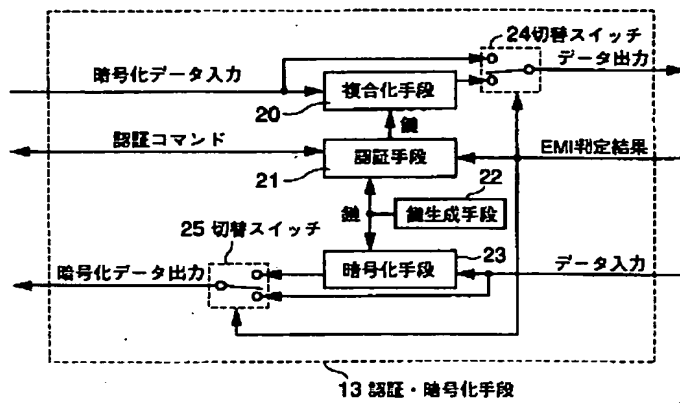
【図1】



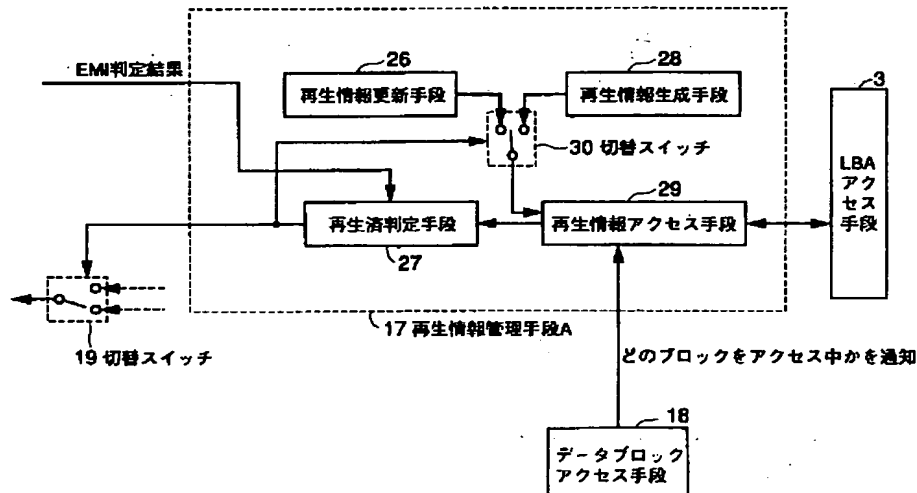
【図2】



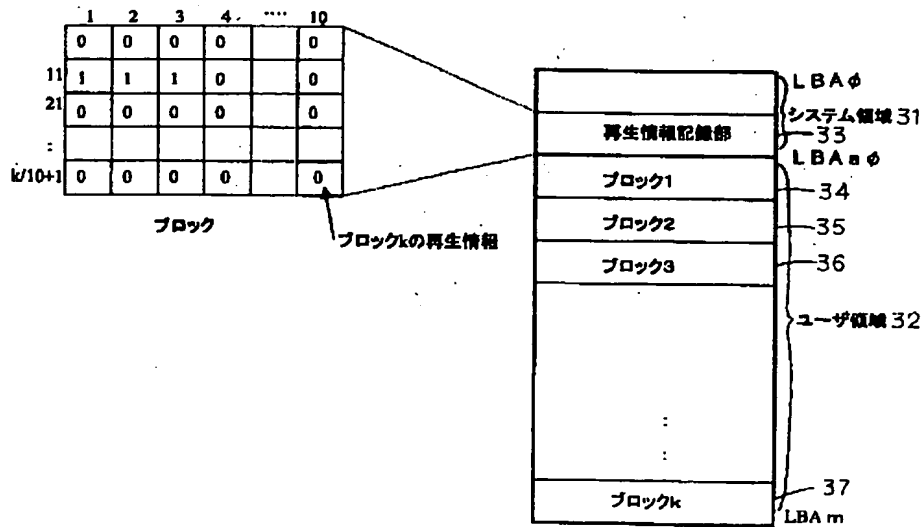
【図3】



【図4】

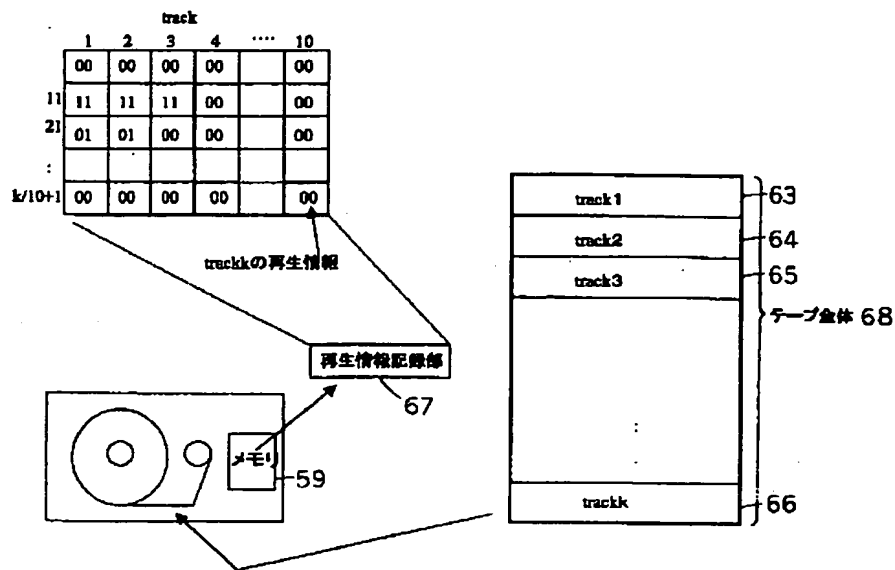


【図5】

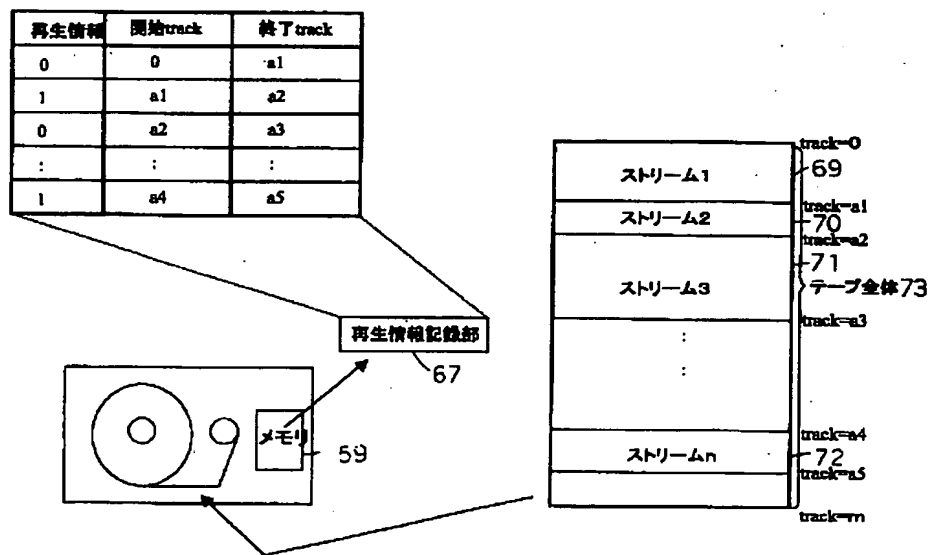


	LBAφ	
再生情報記憶部	システム領域 38	
	40	LBA aφ
ストリーム1	41	
ストリーム2	LBA=a1	
	42	LBA=a2
ストリーム3	43	ユーザ領域 39
		LBA=a3
:		
:		
ストリームn	LBA=a4	
	44	LBA=a5
		LBA=m

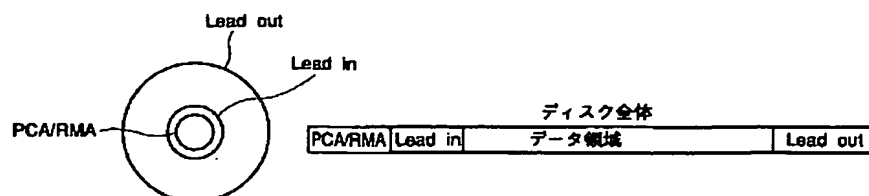
【図14】



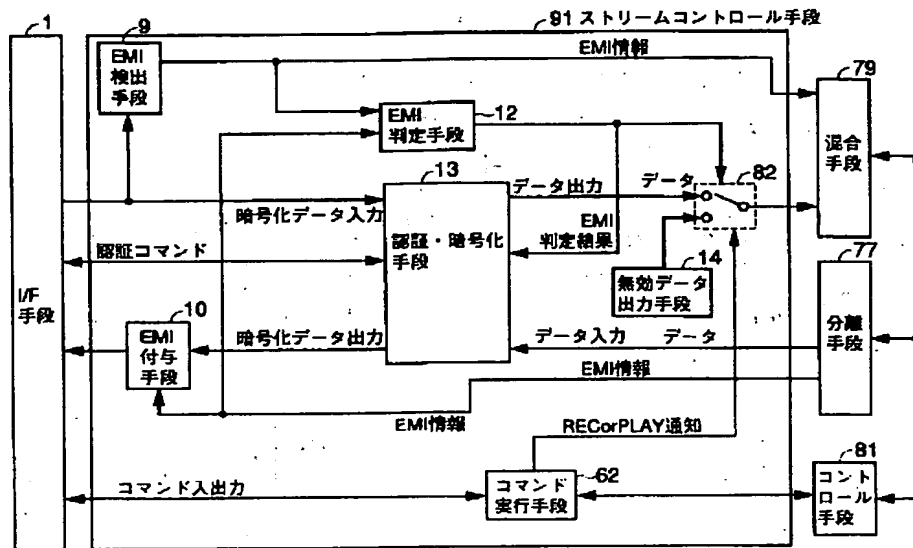
【図15】



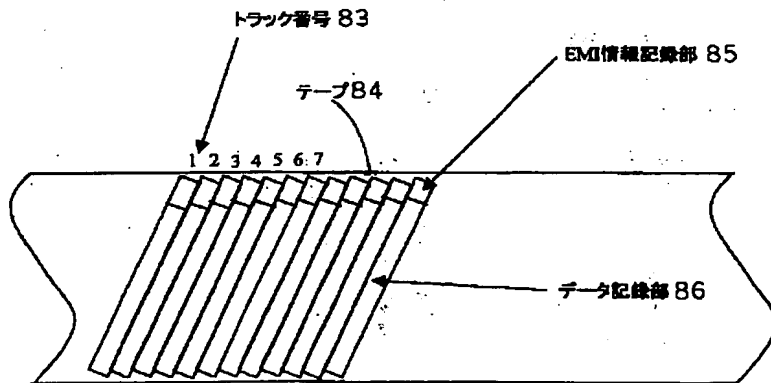
【図24】



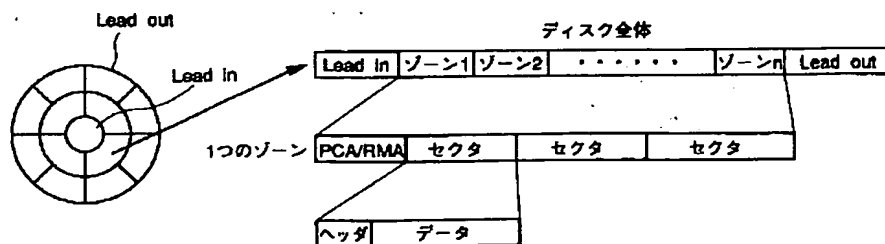
【図17】



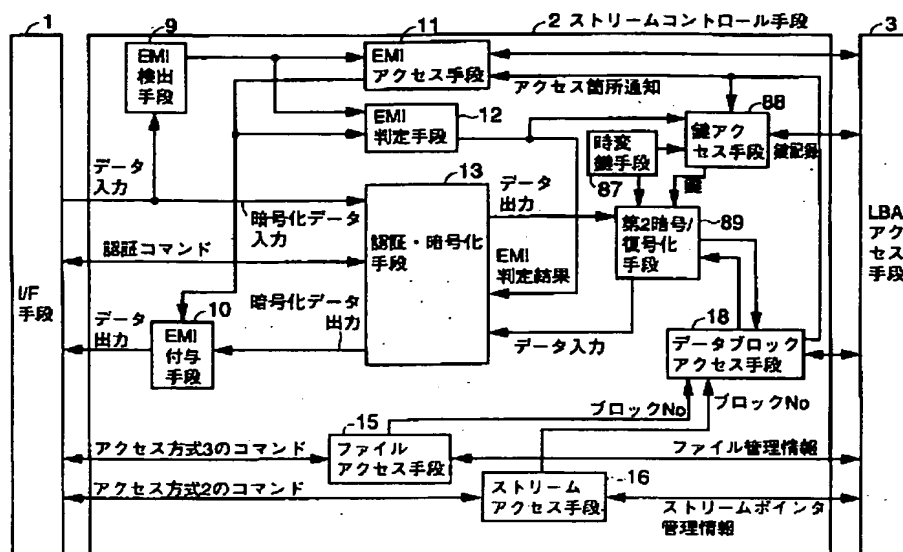
【図18】



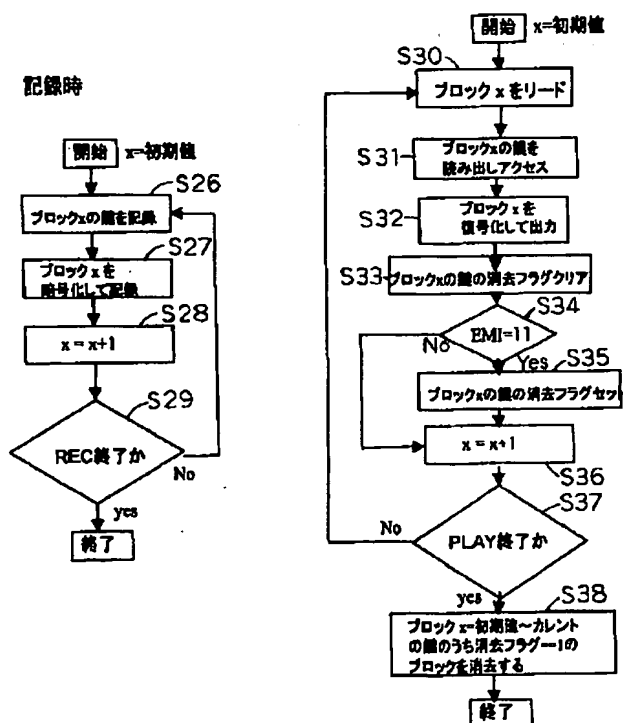
【図25】



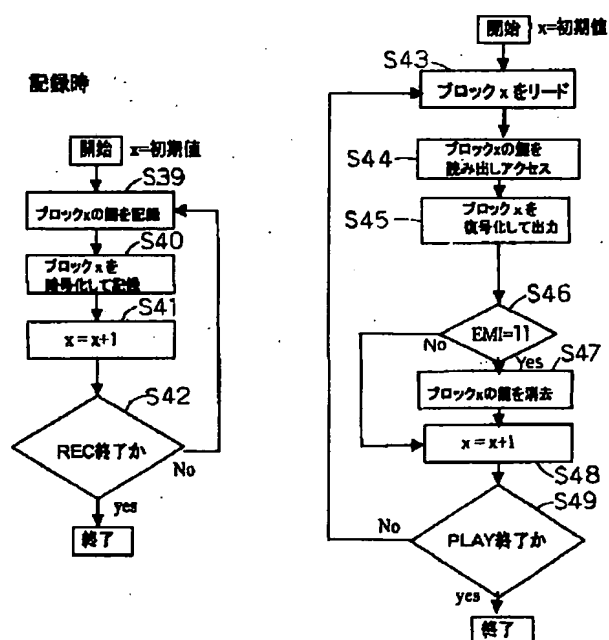
【図19】



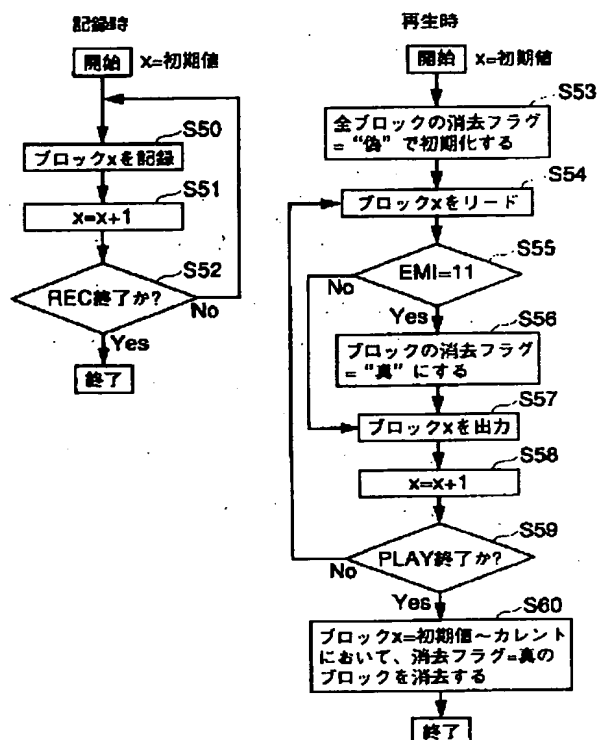
【図20】



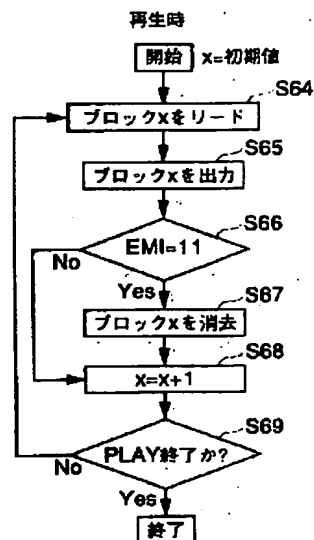
【図21】



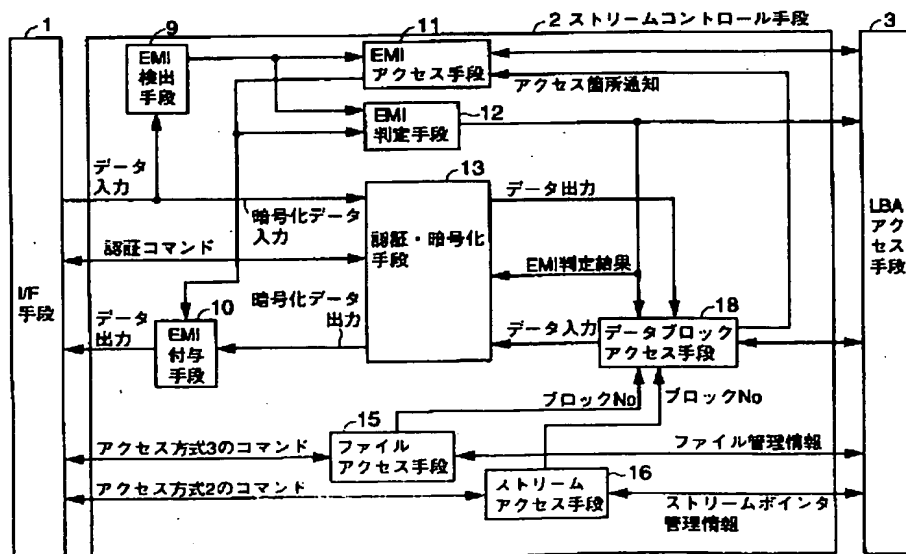
【图 2 2】



【图 2 3】



【图 26】



フロントページの続き

(51)Int.Cl. ⁷	識別記号	FI	テームト* (参考)
H04L 9/32		H04L 9/00	675A
(72)発明者 武知 秀明		(72)発明者 後藤 昌一	
大阪府門真市大字門真1006番地 松下電器		大阪府門真市大字門真1006番地 松下電器	
産業株式会社内		産業株式会社内	
(72)発明者 山田 正純		Fターム(参考) 5B017 AA06 AA07 BA05 BA07 BB03	
大阪府門真市大字門真1006番地 松下電器		BB10 CA06 CA07 CA09 CA11	
産業株式会社内		CA16	
(72)発明者 飯塚 裕之		5B065 BA01 CA11 PA04	
大阪府門真市大字門真1006番地 松下電器		5D044 AB05 AB07 BC01 BC02 CC03	
産業株式会社内		CC04 DE50 GK12 GK17 HL08	
		HL11	
		5J104 AA13 BA03 EA09 EA16 NA02	
		NA27 PA14	